Editors: José Luís da Cruz Vilaça, Rita Leandro Vasconcelos,
Miguel Gorjão-Henriques and Alberto Saavedra

The internal market and the digital economy

XXVIII FIDE CONGRESS
Lisbon/Estoril
(23-26 May 2018)
Congress Proceedings
Vol. 1



ALMEDINA

The internal market and the digital economy

Le marché intérieur et l'économie digitale

Der Binnenmarkt und die digitale Wirtschaft

The internal market and the digital economy

Le marché intérieur et l'économie digitale

Der Binnenmarkt und die digitale Wirtschaft

CONGRESS PROCEEDINGS VOL.1

Editors:
José Luís da Cruz Vilaça, Rita Leandro Vasconcelos,
Miguel Gorjão-Henriques and Alberto Saavedra

ALMEDINA

THE INTERNAL MARKET AND THE DIGITAL ECONOMY
LE MARCHÉ INTÉRIEUR ET L'ÉCONOMIE DIGITALE
DER BINNENMARKT UND DIE DIGITALE WIRTSCHAFT

COORDENAÇÃO
José Luís da Cruz Vilaça, Rita Leandro Vasconcelos,
Miguel Gorjão-Henriques and Alberto Saavedra
EDITOR
EDIÇÕES ALMEDINA, S.A.
Rua Fernandes Tomás, nºs 76-80
3000-167 Coimbra
Tel.: 239 851 904 · Fax: 239 851 901
www.almedina.net · editora@almedina.net
DESIGN DE CAPA
FBA.
PRÉ-IMPRESSÃO
João Jegundo
IMPRESSÃO E ACABAMENTO

Maio, 2018
DEPÓSITO LEGAL

Os dados e as opiniões inseridos na presente publicação são da exclusiva responsabilidade do(s) seu(s) autor(es).
Toda a reprodução desta obra, por fotocópia ou outro qualquer processo, sem prévia autorização escrita do Editor, é ilícita e passível de procedimento judicial contra o infrator.



BIBLIOTECA NACIONAL DE PORTUGAL – CATALOGAÇÃO NA PUBLICAÇÃO

XXVIII FIDE Congress – Lisbon/Estoril (23-26 May 2018)

FIDE (Fédération Internationale pour le Droit Européen / International Federation for European Law)
XXVIII FIDE Congress; [org.] APDE (Associação Portuguesa de Direito Europeu). – 3 v.
V. 1: p. – ISBN 978-972-40-7478-8
Editors: José Luís da Cruz Vilaça, Rita Leandro Vasconcelos, Miguel Gorjão-Henriques and Alberto Saavedra

CDU 34

High Patronage

COM O ALTO PATROCÍNIO
DE SUA EXCELÊNCIA

UNDER THE HIGH PATRONE OF THE
PRESIDENT OF THE PORTUGUESE REPUBLIC

O Presidente da República

Institutional Supporters

CVRIA

European Commission

AUTORIDADE DA CONCORRÊNCIA
PORTUGUESE COMPETITION AUTHORITY

CASCAIS
The Charm of the Atlantic Coast

Marinha

FUNDAÇÃO CALOUSTE GULBENKIAN

UNIVERSIDADE NOVA DE LISBOA

REPÚBLICA PORTUGUESA
CULTURA

PATRIMÓNIO CULTURAL
Direção-Geral do Património Cultural

MNAA
MUSEU NACIONAL DE ARTE ANTIGA

Palácio Nacional da Ajuda

MOSTEIRO DOS JERÓNIMOS

Museu Nacional dos Coches

jurisnova
Associação da Faculdade de Direito da Universidade Nova de Lisboa

Premium Sponsors

CASINO ESTORIL

ctt

edp

Jerónimo Martins

Santander

Premium Partners

ABREU ADVOGADOS

CUATRECASAS

GARRIGUES

GA_P
Gómez-Acebo & Pombo

Linklaters

Luís Silva Morais
Sérgio Gonçalves do Cabo
& Associados, SP, RL
Sociedade de Advogados

MORAIS LEITÃO
GALVÃO TELES
SOARES DA SILVA

PLMJ
ADVOGADOS, SP, RL
50 YEARS
By your side.

SOCIEDADE DE ADVOGADOS, SP, RL
ROGÉRIO FERNANDES FERREIRA
& ASSOCIADOS

URÍA MENÉNDEZ
PROENÇA DE CARVALHO

VdA VIEIRA DE ALMEIDA

Congress Partners

C/M/S/ Rui Pena & Arnaut

Sérvulo & Associados | Sociedade de Advogados, SP, RL

SRS ADVOGADOS
25
CREATING VALUE
1992-2017

TELLES
TELLES DE ABREU | ADVOGADOS

Other Sponsors and Contributors

FIDELIDADE
SEGUROS DESDE 1808

glintt

hmR
HEALTH MARKET RESEARCH

SONAE

Wolters Kluwer

General Rapporteur:

Peggy Valcke

Institutional Rapporteur:

Piedade Costa de Oliveira

Editors:

**José Luís da Cruz Vilaça, Rita Leandro Vasconcelos,
Miguel Gorjão-Henriques and Alberto Saavedra**

Members of the board of APDE
(Portuguese Association for European Law):

**José Luís da Cruz Vilaça, Carlos Botelho Moniz, Nuno Piçarra,
Rita Leandro Vasconcelos, João Paulo Teixeira de Matos,
Nuno Ruiz and Miguel Gorjão-Henriques**

Executive Committee:

**Alberto Saavedra, Joana Schmid Moura, João de Lemos Portugal,
Filipa Pimentel, Leonor Bettencourt Nunes,
Margarida Rosado da Fonseca, Margarida Sameiro,
Piedade Castro e Sousa and Teresa Côrte-Real**

INTRODUCTION



INTRODUCTION

I. The XXVIII FIDE Congress in Estoril

It is not for nothing that Estoril, situated on the coast of the Atlantic Ocean and at the westernmost point of continental Europe, is the splendid venue of the XXVIII FIDE Congress. At the time when Lisbon was, during the Second World War, one of the most desired destinations for those trying to escape the slaughter ravaging the European continent, Estoril became the vibrant center of secret diplomacy as well as the preferred *lieu d'exil* for crowned heads and dignitaries. Nowadays, being on the outer edge of the European Union, Estoril's location again demonstrates the symbolic value of the region. It is not only a gateway to Europe and European values, represented to a large extent by European law, but it is also a platform from which to see beyond local issues. Just as in previous centuries, when the Portuguese coast served Vasco da Gama and Cabral as a starting point to set sail on their expeditions, we too are now embarking, as lawyers and academics, on an arduous journey that should lead the current reflection on European law to face the internal and external challenges of the Union – nowadays perhaps more than ever before.

Given the profile and location of the XXVIII FIDE Congress, it is not surprising that the organisation of this event has been entrusted to the Portuguese Association for European Law (APDE), which was created in 1984 with the aim of contributing to the dissemination of European law in Portugal. At the same time the APDE, in its capacity as a member of the FIDE, ensures the connection of the Portuguese legal community to the ongoing debate about the most important topics of the European Union.

II. FIDE

Since 1961, FIDE (Féderation Internationale pour le Droit Européen / International Federation for European Law) has brought together the European law

associations of each Member State, of candidate countries, as well as those of Norway and Switzerland.[1] For the last 50 years of its existence, as the common umbrella organization, it has been universally recognized by the international legal community as having a remarkable influence on the development and shaping of both the context and the culture of European Union law. The biennial FIDE Congresses gather several hundred lawyers and professionals from different backgrounds. They are the most important event of reflection and dialogue on EU law and policies, as regards both the legislative and policy developments in the European Union and their application by the EU and national courts. Together with their related publications, the reports compiled by FIDE, published in rich and dense volumes full of information and reflection, the Congresses generate an invaluable treasury of academic writing and debate; landmarks in the study of the core themes in European law and the case law of the Court of Justice of the EU, widely consulted by academics, practitioners and judges.[2]

Previous FIDE Congresses, hosted by numerous European national, cultural and academic capitals, have covered a vast gamut of fundamental and economic topics of vital interest for the European Union.[3] The last Congress in Budapest in 2016 put a special emphasis on the problems of European banking union, private enforcement and collective redress in European competition law, as well as on the division of competences and regulatory powers between the European Union and the Member States. All the chosen topics have been comprehensively analysed and discussed. This time, the XXVIII Congress in Estoril aims to go beyond, and significantly develop, the previous work. The adaptability of the thematic scope of the FIDE's Congresses and publications to the current political and economic context constitutes its distinctive feature.

Beside the unquestionable pertinence of the choice of topics, one of the greatest values of FIDE seems to be its well-established, varied and multilevel dimension. It is not only an organisational structure. It is an institutionalised federation of legal experts – *Great Minds of European Law*[4], empowered to shape its norma-

[1] Statute of the FIDE is available at https://www.fide-europe.org/xms/files/ABOUT_FIDE/Statutes_of_FIDE_FIDE_V3.pdf (10.4.2018).

[2] See Julia Laffranque, FIDE – Uniting Great Minds of European Law: 50 years of the International Federation of European Law, Juridica International XVIII/2011, pp. 173-181; Alexandre Bernier, Constructing and Legitimating: Transnational Jurist Networks and the Making of a Constitutional Practice of European Law, 1950-1970, in Contemporary European History, 2012, pp. 399-415

[3] For more information concerning previous and current FIDE Congresses see https://www.fide-europe.org/Congresses/ (10.4.2018).

[4] Julia Laffranque, op.cit., pp. 173-181, pp. 173-181. The expression, coined by Professor Julia Laffranque, served as a basis of the motto of the XXVI FIDE Congress ('FIDE – Uniting Great Minds of EUropean Law'). Its modified version has also been used by the authors of the Introduction to the XXVI FIDE Congress Publication – Professor Ulla Neergaard, Professor Catherine Jacqueson, Commissioner Nina

tive and cultural framework. As a research tool in understanding the diversity of legal reality, the Congresses and the publication of the results allow experts to share the knowledge they have gained, including with the younger generation of scholars in the PhD seminars. In this regard FIDE is where expertise and dialogue meet head on.

With such an important *spiritus movens* as the development of European legal culture and identity, FIDE is also burdened with responsibility. In times of numerous challenges facing the European Union, it undertakes to fulfil its difficult tasks as well as it can. The XXVIII Congress in Estoril, along with the present publication, serve as a preeminent example of how FIDE can fulfil its noble objectives.

III. Topics

As is the custom, for each of the three topics of the current FIDE biennial work, a questionnaire has been prepared by the General Rapporteur, who also undertakes the responsibility of coordinating the national reports, which have been drafted by experts appointed by the national associations of FIDE. All these reports, together with the general reports prepared by the General Rapporteurs, and accompanied by institutional reports drafted by representatives of the EU institutions, constitute the subject of the present collection.

The themes of the XXVIII Congress have been carefully chosen, accordingly to their general interest, topicality, relevance for the process of European integration and practical ability to attract the participants and a wider audience. '*World peace cannot be safeguarded without the making of creative efforts proportionate to the dangers which threaten it*'[5] – these words, uttered by Robert Schuman in 1950, are still up-to-date. The current necessity to balance openness and safety in the field of European law and policy provides a particular justification for the selection of this year's topics.

1. The internal market and the digital economy[6]

In the new digital era, the economy of new media may be considered as the single most important driver of innovation, competitiveness and growth in Europe and

Holst-Christensen, Professor Jens Hartig Danielsen and Professor Grith Skovgaard Ølykke who adopted it for one of the headlines ('A Collaboration of Great Minds of EUropean Law') in order to stress the relationship between EU law and European law.

[5] Robert Schuman Declaration, 9 May 1950.

[6] General Rapporteur: Professor Peggy Valcke, KU Leuven – CiTiP (Centre for IT & IP Law) – imec (BE), visiting professor at Tilburg University (NL) and Bocconi University Milan (IT). Institutional Rapporteur: Professor Piedade Costa de Oliveira, member of the Legal Service of the European Commission, visiting professor at University of São Paulo (Brazil).

the world. Internet and e-commerce, the new sharing economy and peer-to-peer transactions, not to mention media and telecoms across the borders, are thus at the heart of the discussion and of legislative initiatives at the national and European level. The issue of governance in the digital single market has also become one of the Commission's main priority policy areas for 2014-2019, illustrated by the Digital Single Market Strategy of May 2015[7]. Following its assumptions, the present topic includes in the first place the better access by consumers and businesses to new markets, online goods and services across Europe. In this regard, the necessity to eliminate key differences between the online and offline worlds and hence to remove obstacles to cross-border activity is of the highest importance. Second, the examination of the topic will address the development of the appropriate conditions for digital network and services. A particular emphasis has been placed on high-speed, secure and reliable infrastructures and content services, as well as on the tailor-made regulatory conditions for innovation, investment, fair competition and a level playing field. The final objective was to discuss the potential for growth of the digital economy in Europe, by analysing the desirability of investment in ICT infrastructures, cloud computing and Big Data, research innovation, accuracy of public services and industrial effectiveness.

Besides the study of the digital single market, its infrastructure and electronic commerce, the topic focuses on the existing and recently amended legal instruments, which cannot in turn be dissociated from the necessary protection of consumers, personal data and fundamental rights – freedom of expression and the right to privacy – information mass storage, confidentiality of communications and global security. Judicial review and the increasing case law on these matters are at the core of reflections on the topic.

As the general report shows, the major problem in this area is the risk of over-regulation in what is a highly changeable and unpredictable field. As such, it requires well-coordinated regulatory instruments but cannot ignore the growing diversity of the relevant activities. From the institutional perspective, it seems important, however, to point out the tendency of the Union legislature in all the above-mentioned areas to resort to regulations as a harmonisation tool, which seems to illustrate the political will to adopt uniform rules within the European Union.

2. Taxation, state aid and distortions of competition[8]

According to the existing case law on tax schemes and State aid, the problems of the tax rulings and their influence on competition, as well as the outcome of the

[7] COM (2015) 192 final.

[8] General Rapporteur: Professor Raymond Luja, Maastricht University (NL), fiscal state aid counsel to Loyens & Loeff N.V., Amsterdam (NL). Institutional Rapporteurs: Ms. Julia Rapp and Ms. Ramona Ianus of European Commission.

Commission's investigations, and pending or future Court's proceedings, are of the utmost importance for the current internal market legal policy. In this regard the present topic encompasses the relationship between such notions as profit shifting and harmful tax competition, double taxation and double non-taxation, including the OECD model instruments. It also provides an insight into the territorial reach of such dealings and remedies.

As the general report shows, both national and international tax systems still suffer from shortcomings, in practice substituting tax harmonization by State aid rules. The growing awareness of the case law and the learning-by-doing processes within the Commission nonetheless seem to be improving the effectiveness of the State aid regime. In the light of the fact that the future of unconditional tax exceptions in the European Union is being questioned, as well as the success of anti-tax avoidance legislation, the need for advance tax rulings is about to increase. From the institutional point of view, the role of the Commission is prominent in this respect, but it can only properly be played on the basis of guidance provided by the Court of Justice of the European Union.

3. The external dimension of the EU policies: horizontal issues; trade and investment; Playstation and asylum[9]

Last but not least, the external aspects of European policies merit our close attention. The evolution of the international community in times of political and military tensions, which have already given rise to significant human and social costs that are dramatically affecting future European Union policies, deserves to be urgently addressed by respected European and international figures.

First of all, an update on the division of powers and competences between the EU institutions and Member States and their respective roles on the international sphere will be required. This would provide a deep follow-up and focused analysis on one aspect that was addressed in the context of topic III in the Budapest XXVII Congress. Secondly, the topic focuses on the international agreements currently being negotiated by the European Union on trade liberalization, market access and investment protection, such as TTIP and CETA, within the context of other regional or global international agreements.[10] In the light of

[9] General Rapporteurs: Professor Christine Kaddous, Université de Genève (CH), visiting professor at the College of Europe (BL/PL) and at Université Paris II Panthéon-Assas (FR); Professor Nuno Piçarra, Professor at the Law Faculty of the Nova University of Lisbon; member of the Academic Network for Legal Studies on Immigration and Asylum in Europe (*Odysseus*) and of the management board of the European Union Agency for Fundamental Rights. Institutional Rapporteurs: Mr. Hubert Légal and Mr. Álvaro de Elera, Legal Service of the Council; Mr. Freddy Drexler and Mr. Anders Neergaard, Legal Service of the European Parliament.

[10] At the time of writing, the rapporteurs did not have access to the Court of Justice judgment in Case C-284/16, *Slovak Republic v. Achmea BV*. In its preliminary ruling of 6 March 2018, the Court concluded

recent case law of the Court of Justice, the institutional report considers mixed agreements as a political choice for the Union legislature and, in this context, raises the question of the conditions of recourse to this type of agreement. In relation to international agreements, the report also reveals the urgent need to strengthen the mechanisms of democratic scrutiny within the European Union institutions and Member States.

On the other hand, the immense challenges of immigration and asylum that our Area of Freedom, Security and Justice is facing will provide the opportunity for an intense debate. It is crucial to understand how the current crisis is impacting, or will impact, on the existing and evolving regulations, international agreements, practices and institutional machinery dealing with such fundamental issues, including judicial protection and the rule of law. It is our firm belief that the European Union is a unique framework to achieve all those objectives while respecting fundamental rights, democracy and the rule of law. The preservation of these values for the next generations of European citizens is one of the most important objectives of our times.

4. Further debates

In order to give a wider insight on the debate, an introductory panel on *Europe at the Crossroads* has been scheduled. In their opening lectures, Professor Catherine Barnard and Professor Michael O'Flaherty will discuss respectively 'The future of Europe post-Brexit' and 'Fundamental rights as a road sign at the crossroads'. This panel should provide an excellent starting point for the debate led by the prominent speakers in the panel on *Europe and Brexit,* concerning one of the most traumatic events in the current history of the European Union.

IV. Acknowledgments

As President and Members of the Board of the Portuguese Association for European Law (APDE – Associação Portuguesa de Direito Europeu), we would like to thank His Excellency the President of the Portuguese Republic and His Excellency the Prime Minister of Portugal for the institutional support given to the XXVIII FIDE Congress, organised by APDE in Estoril from 23 to 26 May 2018.

We would also like to express our gratitude to all the rapporteurs, speakers, chairpersons, moderators and interpreters involved in the work of the Congress and of the present publication.

that the arbitration clause in the Agreement between the Netherlands and Slovakia (intra-EU BIT) on the protection of investments is not compatible with EU law. The ruling raises further questions concerning arbitration in the European Union in Investor-State Dispute Settlement.

The organisation of the XXVIII FIDE Congress would not have been possible without the generous contribution of our sponsors and supporters.

The support of the Court of Justice of the European Union and of the European Commission was also of the utmost importance for the success of the Congress.

Last but not least, we would like to thank the members of the Executive Committee of the Congress, Alberto Saavedra, Filipa Pimentel, Joana Schmid Moura, João de Lemos Portugal, Leonor Bettencourt Nunes, Margarida Rosado da Fonseca, Margarida Sameiro, Piedade Castro e Sousa and Teresa Côrte-Real. Without their unconditional dedication to the Congress, its organisation would not have been possible.

José Luís da Cruz Vilaça, Carlos Botelho Moniz, Nuno Piçarra, Rita Leandro Vasconcelos, João Paulo Teixeira de Matos, Nuno Ruiz, Miguel Gorjão-Henriques

INTRODUCTION

I. Le XXVIIIe Congrès de la FIDE à Estoril

Non sans raison, c'est à Estoril, située sur la côte de l'océan Atlantique et à l'extrême ouest de l'Europe continentale, que se tient le XXVIIIe Congrès de la FIDE (Fédération Internationale pour le Droit Européen). À l'époque où Lisbonne était, pendant la Seconde Guerre mondiale, l'une des destinations les plus recherchées par ceux qui tentaient d'échapper au carnage qui ravageait le continent européen, Estoril devint le centre d'une diplomatie secrète effervescente et le lieu d'exil des têtes couronnées et dignitaires. De nos jours, se trouvant à la lisière de l'Union Européenne, la localisation d'Estoril atteste à nouveau du caractère symbolique de la région. Estoril n'offre pas seulement une porte d'entrée vers l'Europe et les valeurs européennes, représentées en grande partie par le droit de l'Union européenne, mais permet également de prendre de la hauteur de vue pour se projeter et /réfléchir au-delà des problèmes locaux. Comme des siècles auparavant, lorsque Vasco de Gama et Cabral partirent de la côte portugaise pour leurs expéditions, nous embarquons maintenant, en tant que juristes et universitaires, dans un périple difficile qui devrait aider la réflexion actuelle sur le droit de l'Union européenne à faire face aux défis internes et externes de l'Union, toujours plus prégnants. Compte tenu du programme et de la localisation du XXVIIIe Congrès de la FIDE, il n'est pas surprenant que son organisation ait été confiée à l'Association portugaise pour le droit européen (APDE), créée en 1984 dans le but de contribuer à la diffusion du droit européen au Portugal. L'APDE, en qualité de membre de la FIDE, est un lieu de débat renouvelé pour la communauté juridique portugaise sur les sujets les plus importants de l'Union européenne.

II. FIDE

Depuis 1961, la FIDE unit les associations de droit européen de chaque État membre, des pays candidats à l'adhésion, ainsi que de la Suisse et la Norvège[1]. En 50 ans d'existence, elle a été reconnue par la communauté juridique internationale comme ayant une influence remarquable sur la formation et le développement d'un cadre européen tant juridique que culturel. Les congrès biennaux de la FIDE réunissent plusieurs centaines de juristes venant d'horizons divers. Ils constituent le point d'orgue de la réflexion et du dialogue sur le droit et les politiques de l'Union, tant en ce qui concerne leur évolution que leur application par les juridictions nationales et européennes. Ensembles avec les congrès, les publications afférentes – les riches et denses Rapports préparés et publiés par la FIDE – constituent de précieux points de repère dans l'étude des thèmes fondamentaux du droit de l'Union et de la jurisprudence de la Cour de justice, largement utilisés par les universitaires, les praticiens et les juges[2].

Les congrès précédents de la FIDE, ayant eu lieu en plusieurs capitales nationales, culturelles et académiques de l'Europe, couvraient un large éventail de sujets juridiques et économiques présentant un intérêt vital pour l'Union européenne[3]. Le dernier Congrès de Budapest en 2016 a mis l'accent sur les problèmes de l'union bancaire européenne, l'exécution privée et les recours collectifs dans le droit européen de la concurrence, ainsi que sur la répartition des compétences et des pouvoirs réglementaires entre l'Union européenne et les États membres. Tous les thèmes choisis ont été analysés et discutés de manière approfondie. Se situant dans la même lignée, le XXVIIIe Congrès d'Estoril vise à approfondir le travail précédent. L'adéquation des thématiques des congrès et des publications de la FIDE au contexte politique et économique actuel constitue son trait distinctif.

Outre la pertinence incontestable du choix des sujets, l'un des plus grands atouts reconnu de la FIDE réside dans la multiplicité et de la diversité de son approche. Loin d'être une simple structure organisationnelle, elle constitue une fédération institutionnalisée d'experts juridiques – les *Grands esprits du droit Européen*[4] – à même d'orienter le cadre culturel et normatif de l'Union. Les études

[1] Statut de la FIDE est disponible sur : https://www.fide-europe.org/xms/files/ABOUT_FIDE/Statutes_of_FIDE_FIDE_V3.pdf (10.4.2018).

[2] Voir Julia Laffranque, FIDE – Uniting Great Minds of European Law: 50 years of the International Federation of European Law, Juridica International XVIII/2011, pp. 173-181; Alexandre Bernier, Constructing and Legitimating: Transnational Jurist Networks and the Making of a Constitutional Practice of European Law, 1950-1970, in Contemporary European History, 2012, pp. 399-415.

[3] Pour plus d'informations sur les congrès précédents et actuels de la FIDE, voir : https://www.fide-europe.org/congresses/ (10.4.2018).

[4] Julia Laffranque, op.cit., pp. 173-181. L'expression, créée par le professeur Julia Laffranque, a servi de base à la devise du XXVIe Congrès de la FIDE ('FIDE – Uniting Great Minds of EUropean Law'). Sa version modifiée a également été utilisée par les auteurs de la Publication accompagnant le Congrès de

juridiques comparatives, en tant qu'outil de recherche pour appréhender la réalité juridique dans sa complexité, la publication de ces travaux, ainsi que les congrès aident les experts à partager les connaissances acquises avec les autres, y compris avec la jeune génération pendant les Séminaires Doctoraux. À cet égard, la FIDE est l'endroit où l'expertise et le dialogue se réunissent.

En tant que *spiritus movens* du développement de la culture et de l'identité juridique européenne, la FIDE a également une responsabilité importante. Au moment où l'Union européenne est confrontée à de nombreux défis, la FIDE parvient, avec succès, à accomplir les missions qui sont les siennes. Le XXVIIIe Congrès d'Estoril, ainsi que la présente publication, en sont la parfaite illustration.

III. Thèmes

Comme le veut la tradition, pour chacun des trois thèmes des travaux de la FIDE, un questionnaire a été préparé par le Rapporteur général, auquel il incombe également de coordonner les rapports nationaux, rédigés par des experts des associations nationales membres de la FIDE. Ces rapports ainsi que les rapports généraux préparés par les rapporteurs généraux et accompagnés des rapports institutionnels élaborés par les représentants des institutions de l'Union, composent le présent ouvrage.

Les thèmes du XXVIIIe Congrès ont été choisis avec soin, en fonction de leur pertinence pour le processus d'intégration européenne, de l'actualité et de leur faculté à attirer de nombreux participants. « *La paix mondiale ne saurait être sauvegardée sans des efforts créateurs à la mesure des dangers qui la menacent.* »[5] – ces mots, prononcés par Robert Schuman en 1950, sont toujours d'actualité. La nécessité de trouver, au regard du droit et des politiques de l'Union européenne, un équilibre entre ouverture et sécurité permet d'aborder de façon particulièrement stimulante les sujets suivants :

1. Le marché intérieur et l'économie digitale[6]

Dans la nouvelle ère numérique, l'économie peut être considérée comme le moteur le plus important de l'innovation, de la compétitivité et de la croissance en Europe et dans le monde. L'Internet et le commerce électronique, la nouvelle

la XXVI de la FIDE – le professeur Ulla Neergaard, le professeur Catherine Jacqueson, le commisseur Nina Holst-Christensen, le professeur Jens Hartig Danielsen et le professeur Grith Skovgaard Ølykke qui l'ont adoptée pour l'un des titres de l'Introduction ('A Collaboration of Great Minds of EUropean Law') afin de souligner la relation entre le droit de l'UE et le droit européen.

[5] Déclaration de Robert Schuman, 9 mai 1950.

[6] Rapporteur général: Professeur Peggy Valcke, KU Leuven – CiTiP (Centre for IT & IP Law) – imec (BE), professeur invité à l'Université de Tilburg (NL) et à l'Université Bocconi de Milan (IT). Rapporteur institutionnel: Professeur Piedade Costa de Oliveira, membre du service juridique de la Commission européenne, professeur invité à l'Ecole Polytechnique de l'Université de São Paulo (Brésil).

économie du partage et les transactions *peer-to-peer,* sans oublier les médias et les télécommunications par-delà les frontières, sont ainsi au cœur de la discussion et des initiatives législatives au niveau national et européen. La question de la gouvernance dans le marché unique numérique est devenue l'un des principaux domaines d'action prioritaires de la Commission pour la période 2014-2019, illustrée par la Stratégie pour un marché unique numérique en mai 2015[7]. Suivant les hypothèses de cette Stratégie, le présent sujet suppose, en premier lieu, de réfléchir à un meilleur accès des consommateurs et des entreprises à de nouveaux marchés, biens et services en ligne à travers l'Europe. À cet égard, la nécessité d'éliminer les différences principales entre les mondes *on-line* et *off-line* pour mettre fin aux obstacles à l'activité transfrontalière est de la plus haute importance. En second lieu, le présent sujet porte sur des conditions adéquates pour le développement du réseau et des services numériques. Un accent particulier a été mis sur les infrastructures et les services en ligne rapides, sécurisés et fiables, ainsi que sur les conditions réglementaires appropriées aux innovations, à la concurrence loyale, à l'investissement et aux conditions de concurrence équitable. L'objectif final est de discuter du potentiel de croissance de l'économie numérique en Europe, en analysant la nécessité d'investir dans les infrastructures TIC, le *Cloud computing* et le *Big Data*, l'innovation dans la recherche, la pertinence des services publics ainsi que l'efficacité industrielle.

Outre l'étude du marché unique numérique, de ses infrastructures et du commerce électronique, les réflexions, ciblées sur des instruments juridiques existants et récemment révisés, ne peuvent être dissociées de l'objectif de protection des consommateurs, des données personnelles et des droits fondamentaux, comme l'illustre la nécessité de préserver la sécurité, la liberté d'expression et la confidentialité des communications face au le stockage de masse des informations Le contrôle judiciaire et la jurisprudence croissante sur ces questions sont au cœur de la réflexion proposée .

Comme le montre l'étude générale, le problème majeur du thème analysé concerne le risque d'une réglementation excessive dans une matière mouvante et imprévisible. En tant que tel, l'encadrement de l'économie numérique nécessite des instruments réglementaires adaptés et bien coordonnés. D'un point de vue institutionnel, il semble intéressant de souligner la tendance du législateur européen à appliquer fréquemment dans tous les domaines susmentionnés la réglementation en tant qu'instrument d'harmonisation ce qui semble illustrer la volonté d'adopter des règles uniformes au sein de l'Union européenne.

[7] COM (2015) 192 final.

2. Fiscalité, aides d'État et distorsions de la concurrence[8]

Au regard des problèmes de *tax ruling* et de leur influence sur la concurrence, les résultats des enquêtes de la Commission et l'issue des procédures éventuelles devant la Cour de justice revêtent une importance pressante pour la politique juridique européenne. À cet égard, le présent sujet englobe la relation entre des notions telles que le transfert de bénéfices, la concurrence fiscale dommageable et les conventions visant à éviter une double imposition, y compris les instruments types de l'OCDE, et fournit un aperçu à l'échelle territoriale des problèmes soulevés par ceux-ci.

Comme le montre l'étude générale, les systèmes fiscaux nationaux et internationaux comportent, en l'absence d'harmonisation fiscale, des lacunes. Cette absence d'harmonisation positive est palliée par le recours au droit des aides d'État. La sensibilisation croissante à la jurisprudence et les processus *learning-by-doing* au sein de la Commission semblent toutefois déjà en cours afin d'améliorer l'efficacité du régime des aides d'État. L'avenir des exemptions fiscales inconditionnelles dans l'Union étant remis en cause, de même que le succès des législations nationales anti-évitement et anti-abus, le besoin de décisions anticipées en matière fiscale augmente. Du point de vue institutionnel, le rôle de la Commission est important à cet égard, mais ne peut être joué que sur une base solide fournie par la Cour de justice.

3. La dimension extérieure des politiques de l'Union européenne: questions horizontales; commerce et investissements; immigration et asile[9]

Les aspects externes de la politique européenne devraient également retenir notre attention. Les évolutions au sein de la communauté internationale en période de tensions politiques et militaires, qui ont déjà entraîné des coûts humains et sociaux dramatiques affectant gravement les politiques de l'UE pour les temps à venir, mérite d'être traitée urgemment par d'éminentes personnalités européennes et internationales.

Premièrement, le sujet apporte une mise à jour quant à la répartition des pouvoirs et des compétences entre les institutions de l'Union et les États membres

[8] Rapporteur général: Professeur Raymond Luja, Université de Maastricht (NL), conseiller juridique en matière d'aides d'État auprès de Loyens & Loeff N.V., Amsterdam (NL). Rapporteurs institutionnels: Mme Julia Rapp, Mme Ramona Ianus, Services de la Commission européenne.

[9] Rapporteurs généraux: Professeur Christine Kaddous, Université de Genève (CH), professeur invité au Collège d'Europe (BL/ PL) et à l'Université Paris II Panthéon-Assas (FR); Professeur Nuno Piçarra, Professeur à la Faculté de droit de l'Université Nova de Lisbonne, membre du Réseau académique d'études juridiques sur l'immigration et l'asile en Europe (*Odysseus*) et du Conseil d'administration de l'Agence des droits fondamentaux de l'Union européenne. Rapporteurs institutionnels: M. Hubert Légal et M. Álvaro de Elera, Services juridiques du Conseil; M. Freddy Drexler et M. Anders Neergaard, Services juridiques du Parlement européen.

ainsi que leurs rôles respectifs sur la scène internationale. Il permet ainsi un approfondissement d' un des aspects déjà abordé dans le contexte du thème III du XXVIIe Congrès de Budapest En outre, le thème porte sur les accords internationaux actuellement négociés par l'UE dans le cadre de la libéralisation des échanges, l'accès au marché et la protection des investissements, tels que le TTIP et le CETA[10]. Au regard de la jurisprudence récente de la Cour de justice, le rapport institutionnel appréhende les accords mixtes en tant que choix politique pour le législateur de l'Union et, dans ce cadre, soulève la question des conditions de recours à ce type d'accords. Le rapport révèle également la nécessité urgente de renforcer les mécanismes de contrôle démocratique au sein des institutions européennes et des États membres s'agissant des accords internationaux.

Deuxièmement, les immenses défis en matière d'immigration et d'asile auxquels l'Espace de liberté, de sécurité et de justice est confronté, susciteront un débat intense. Il est essentiel de comprendre comment la crise actuelle affecte ou aura un impact sur les réglementations, les accords internationaux, les pratiques et les mécanismes institutionnels existants et futurs qui traitent des questions fondamentales, notamment la protection judiciaire et le respect du droit. Nous sommes fortement convaincus que l'Union européenne est un cadre unique pour relever ces défis dans le respect des droits fondamentaux, de la démocratie et du droit. La préservation de ces valeurs pour les prochaines générations de citoyens européens est l'un des objectifs les plus importants de notre époque.

4. Questions ouvertes

Afin de contextualiser nos réflexions, un panel introductif relatif à *l'Europe à la croisée des chemins* a été ajouté. Dans leurs interventions d'ouverture, les professeurs Catherine Barnard et Michael O'Flaherty discuteront sur les thèmes suivants : '*The future of Europe post Brexitet* ' et '*The fundamental rights as a road sign at the crossroads*'. Ce panel devrait servir de point de départ à un débat approfondi entre les éminents intervenants du panel sur *l'Europe et le Brexit*, l'un des événements les plus traumatisants de l'histoire récente de l'Union européenne.

IV. Remerciements

En qualité de président et membres du Conseil Directeur de l'Association Portugaise pour le Droit Européen (APDE – Associação Portuguesa de Direito Euro-

[10] Au moment de la rédaction du présent recueil, les rapporteurs n'avaient pas eu accès à l'arrêt de la CJUE du 6 mars 2018 dans l'affaire C-284, *Slovak Republic c. Achmea BV*. En réponse à la question préjudicielle, la Cour de justice a estimé que la clause d'arbitrage de l'accord entre les Pays-Bas et la Slovaquie (intra-UE TBI) sur la protection des investissements n'est pas compatible avec le droit de l'UE. La décision soulève de nombreuses questions concernant l'arbitrage des différends entre investisseurs et États au sein de l'Union.

peu), nous tenons à remercier Son Excellence le Président de la République Portugaise et Son Excellence le Premier Ministre du Portugal pour le soutien institutionnel apporté au XXVIIIème Congrès de la FIDE, que l'APDE a organisé à Estoril du 23 au 26 mai 2018.

Nous souhaitons également exprimer notre reconnaissance à tous les rapporteurs, orateurs, présidents de séance, modérateurs et interprètes qui ont contribué aux travaux du Congrès et de la présente publication. La réalisation du XXVIIIème Congrès de la FIDE n'aurait pas été possible sans la généreuse contribution de nos sponsors et supporters.

Nous souhaitons également mettre en exergue l'importance du soutien de la Cour de justice de l'Union européenne et de la Commission européenne pour le succès de ce Congrès.

Enfin, nous souhaitons remercier tout particulièrement les membres du Comité Exécutif du Congrès, Alberto Saavedra, Filipa Pimentel, Joana Schmid Moura, João de Lemos Portugal, Leonor Bettencourt Nunes, Margarida Rosado da Fonseca, Margarida Sameiro, Piedade Castro e Sousa et Teresa Côrte-Real. Sans leur dévouement inconditionnel au Congrès, l'organisation de celui-ci n'aurait pas été possible.

José Luís da Cruz Vilaça, Carlos Botelho Moniz, Nuno Piçarra, Rita Leandro Vasconcelos, João Paulo Teixeira de Matos, Nuno Ruiz, Miguel Gorjão-Henriques

EINFÜHRUNG

I. Der XXVIII. FIDE-Kongress in Estoril

Nicht umsonst ist Estoril, das sich an der Küste des Atlantischen Ozeans und am westlichsten Punkt Kontinentaleuropas befindet, der prächtige Schauplatz des XXVIII. FIDE-Kongresses. Während des Zweiten Weltkriegs, als Lissabon eines der begehrtesten Ziele war für diejenigen, die dem Massaker auf dem europäischen Kontinent entkommen wollten, wurde Estoril zum pulsierenden Zentrum der Geheimdiplomatie und zum bevorzugten Zufluchtsort für gekrönte Häupter und Würdenträger. Heute befindet sich Estoril am äußersten Rand der Europäischen Union und beweist erneut den symbolischen Wert der Region. Es ist nicht nur ein Tor zu Europa und europäischen Werten, die zu einem großen Teil vom europäischen Recht repräsentiert werden, sondern es ist auch eine Plattform, die die Möglichkeit bietet, über lokale Probleme hinauszublicken. Wie in früheren Jahrhunderten, als die portugiesische Küste Vasco da Gama und Cabral als Ausgangspunkt für ihre Expeditionen diente, begeben wir uns jetzt als Anwälte und Akademiker auf eine beschwerliche Reise, die das aktuelle Nachdenken über das europäische Recht anstoßen sollte, um den internen und externen Herausforderungen der Union ins Auge sehen zu können – heute vielleicht mehr als jemals zuvor.

Angesichts des Profils und des Standorts des XXVIII. FIDE-Kongresses ist es nicht verwunderlich, dass die Organisation dieser Veranstaltung der Portugiesischen Vereinigung für Europäisches Recht (APDE) anvertraut wurde, gegründet 1984 mit dem Ziel, zur Verbreitung des europäischen Rechts in Portugal beizutragen. Gleichzeitig stellt die APDE als Mitglied der FIDE die Verbindung der portugiesischen Rechtsgemeinschaft zur laufenden Debatte über die wichtigsten Themen der Europäischen Union sicher.

II. FIDE

Die FIDE (Fédération Internationale pour le Droit Européen / Internationale Vereinigung für Europarecht) hat seit 1961 die europäischen Rechtsverbände der einzelnen Mitgliedstaaten, der Bewerberländer sowie Norwegens und der Schweiz zusammengeführt[1]. In den letzten 50 Jahren ihres Bestehens wurde sie als gemeinsame Dachorganisation von der internationalen Rechtsgemeinschaft allgemein anerkannt, da sie einen bemerkenswerten Einfluss auf die Entwicklung und Gestaltung sowohl des Kontexts als auch der Kultur des Unionsrechts hat. Die alle zwei Jahre stattfindenden FIDE-Kongresse versammeln mehrere hundert Anwälte und Fachleute mit unterschiedlichem Hintergrund. Sie sind das wichtigste Ereignis der Reflexion und des Dialogs über EU-Recht und -Politik, sowohl was die legislativen als auch die politischen Entwicklungen in der Europäischen Union anbelangt, und ihre Anwendung durch die EU und die nationalen Gerichte. Zusammen mit den entsprechenden Publikationen, den Berichten der FIDE, die in reichen und schweren Bänden voller Information und Reflexion veröffentlicht werden, schaffen die Kongresse eine unbezahlbare Schatzkammer des wissenschaftlichen Schreibens und der Debatte; Orientierungspunkte bei der Untersuchung der Kernthemen des europäischen Rechts und der Rechtsprechung des Gerichtshofs der EU, die von Akademikern, Praktikern und Richtern umfassend konsultiert werden[2].

Frühere FIDE-Kongresse, die von zahlreichen europäischen nationalen, kulturellen und akademischen Hauptstädten veranstaltet wurden, decken ein breites Spektrum grundlegender und wirtschaftlicher Themen ab, die von vitaler Bedeutung für die Europäische Union sind[3]. Der letzte Kongress in Budapest im Jahr 2016 richtete besondere Aufmerksamkeit auf die Probleme der europäischen Bankenunion, die private Durchsetzung und den kollektiven Rechtsschutz im europäischen Wettbewerbsrecht sowie auf die Aufteilung der Zuständigkeiten und Regelungsbefugnisse zwischen der Europäischen Union und den Mitgliedstaaten. Alle ausgewählten Themen wurden ausführlich analysiert und diskutiert. Diesmal will der XXVIII. Kongress in Estoril die bisherige Arbeit übertreffen und deutlich weiterentwickeln. Die Anpassungsfähigkeit des thematischen Rahmens der FIDE-Kongresse und -Veröffentlichungen

[1] Das Statut der FIDE ist verfügbar unter https://www.fide-europe.org/xms/files/ABOUT_FIDE/Statutes_of_FIDE_FIDE_V3.pdf (10.4.2018).

[2] Siehe Julia Laffranque, FIDE – Uniting Great Minds of European Law: 50 years of the International Federation of European Law, Juridica International XVIII/2011, pp. 173-181; Alexandre Bernier, Constructing and Legitimating: Transnational Jurist Networks and the Making of a Constitutional Practice of European Law, 1950-1970, in Contemporary European History, 2012, pp. 399-415.

[3] Weitere Informationen zu früheren und aktuellen FIDE-Kongressen finden Sie unter HYPERLINK "https://www.fide-europe.org/congresses/" https://www.fide-europe.org/Congresses/ (10.4.2018).

an den aktuellen politischen und wirtschaftlichen Kontext macht seine Besonderheit aus.

Neben der unzweifelhaften Relevanz der Themenwahl scheint einer der größten Werte der FIDE ihre gut etablierte, vielfältige und mehrstufige Dimension zu sein. Es ist nicht nur eine Organisationsstruktur. Es ist ein institutionalisierter Verband von Rechtsexperten – Great Minds of European Law[4] mit der Befugnis, seinen normativen und kulturellen Rahmen zu gestalten. Als ein Forschungsinstrument zum Verständnis der Vielfalt der rechtlichen Realität ermöglichen die Kongresse und die Veröffentlichung der Ergebnisse den Experten, ihr erworbenes Wissen zu teilen, auch mit der jüngeren Wissenschaftlergeneration in den PhD-Seminaren. In dieser Hinsicht ist die FIDE der Ort, an dem Fachwissen und Dialog aufeinandertreffen.

Mit einem so wichtigen spiritus movens wie der Entwicklung der europäischen Rechtskultur und -identität trägt die FIDE auch eine gewisse Verantwortung. In Zeiten zahlreicher Herausforderungen für die Europäische Union verpflichtet sie sich, ihre schwierigen Aufgaben so gut wie möglich zu erfüllen. Zusammen mit der vorliegenden Veröffentlichung dient der XXVIII. Kongress in Estoril als herausragendes Beispiel dafür, wie die FIDE ihre edlen Ziele erfüllen kann.

III. Themen

Wie üblich, arbeitete der Generalberichterstatter für jedes der drei Themen der aktuellen zweijährlichen Arbeit der FIDE einen Fragebogen aus. Er übernimmt auch die Verantwortung für die Koordinierung der nationalen Berichte, zusammengestellt von Experten, die von den nationalen FIDE-Verbänden ernannt wurden. Zusammen mit den von den Generalberichterstattern erstellten allgemeinen Berichten und den von Vertretern der EU-Institutionen verfassten institutionellen Berichten bilden alle diese Berichte den Gegenstand der vorliegenden Sammlung.

Die Themen des XXVIII. Kongresses wurden sorgfältig ausgewählt, entsprechend ihrem allgemeinen Interesse, ihrer Aktualität, ihrer Relevanz für den Prozess der europäischen Integration und ihrer praktischen Fähigkeit, die Teilnehmer und ein breiteres Publikum zu gewinnen. „Es wird kaum möglich sein,

[4] Julia Laffranque, aaO, S. 173-181, S. 173-181. Der von Professorin Julia Laffranque geprägte Ausdruck diente als Grundlage für das Motto des XXVI. FIDE-Kongresses („FIDE – Uniting Great Minds of EUropean Law"). Seine modifizierte Version wurde auch von den Autoren der Einführung in die Publikationen des XXVI. FIDE-Kongresses – Professorin Ulla Neergaard, Professorin Catherine Jacqueson, Kommissarin Nina Holst-Christensen, Professor Jens Hartig Danielsen und Professor Grith Skovgaard Ølykke - verwendet, die ihn für eine der Titelzeilen („A Collaboration of Great Minds of EUrepean Law") übernahmen, um das Verhältnis zwischen EU-Recht und europäischem Recht zu betonen.

den Weltfrieden zu erhalten, wenn wir uns nicht auch um neuartige Lösungen bemühen, die den drohenden Gefahren wirklich gerecht werden“[5] – diese Worte von Robert Schuman aus dem Jahr 1950 sind immer noch aktuell. Die derzeitige Notwendigkeit, ein Gleichgewicht zwischen Offenheit und Sicherheit im Bereich des europäischen Rechts und der europäischen Politik herzustellen, ist eine besondere Rechtfertigung für die Auswahl der diesjährigen Themen.

1. Der Binnenmarkt und die digitale Wirtschaft[6]

In der neuen digitalen Ära kann die Wirtschaft der neuen Medien als der wichtigste Motor für Innovation, Wettbewerbsfähigkeit und Wachstum in Europa und der Welt angesehen werden. Internet und E-Commerce, die neue Sharing Economy und Peer-to-Peer-Transaktionen, ganz zu schweigen von Medien und Telekommunikation über die Grenzen hinweg, stehen daher im Mittelpunkt der Diskussion und der legislativen Initiativen auf nationaler und europäischer Ebene. Das Thema der Governance im digitalen Binnenmarkt ist auch zu einem der wichtigsten politischen Schwerpunktbereiche der Kommission für den Zeitraum 2014-2019 geworden, wie die Strategie für einen digitalen Binnenmarkt vom Mai 2015 zeigt[7]. Nach ihren Annahmen umfasst das vorliegende Thema in erster Linie den besseren Zugang von Verbrauchern und Unternehmen zu neuen Märkten, Online-Waren und -Dienstleistungen in ganz Europa. In dieser Hinsicht ist die Notwendigkeit, wesentliche Unterschiede zwischen der Online- und der Offline-Welt aufzuheben und somit Hindernisse für grenzüberschreitende Aktivitäten zu beseitigen, von größter Bedeutung. Zweitens befasst sich die Untersuchung des Themas mit der Entwicklung geeigneter Bedingungen für digitale Netze und Dienste. Ein besonderer Schwerpunkt wurde auf schnelle, sichere und zuverlässige Infrastrukturen und Inhaltedienste sowie auf die maßgeschneiderten Regulierungsbedingungen für Innovation, Investitionen, fairen Wettbewerb und gleiche Wettbewerbsbedingungen gelegt. Das endgültige Ziel bestand darin, das Wachstumspotenzial der digitalen Wirtschaft in Europa zu diskutieren, indem die Attraktivität von Investitionen in IKT-Infrastrukturen, Cloud Computing und Big Data, Forschungsinnovation, Genauigkeit der öffentlichen Dienste und industrielle Effizienz analysiert wurde.

[5] Erklärung von Robert Schuman, 9. Mai 1950.

[6] Generalberichterstatterin: Professorin Peggy Valcke, KU Leuven – CiTiP (Zentrum für IT & IP-Recht) - imec (BE), Gastprofessorin an der Universität Tilburg (NL) und an der Bocconi-Universität Mailand (IT). Institutionelle Berichterstatterin: Professorin Piedade Costa de Oliveira, Mitglied des Juristischen Dienstes der Europäischen Kommission, Gastprofessorin an der Universität São Paulo (Brasilien).

[7] Generalberichterstatter: Professor Raymond Luja, Universität Maastricht (NL), Steuerberater von Loyens & Loeff N.V., Amsterdam (NL). Institutionelle Berichterstatterinnen: Frau Julia Rapp und Frau Ramona Ianus von der Europäischen Kommission.

Neben der Untersuchung des digitalen Binnenmarkts, seiner Infrastruktur und seines elektronischen Handels konzentriert sich das Thema auf die bestehenden und kürzlich geänderten Rechtsinstrumente, die nicht vom notwendigen Schutz der Verbraucher, der personenbezogenen Daten und der Grundrechte – Meinungsfreiheit und Recht auf Privatsphäre – getrennt werden können, Massenspeicherung von Informationen, Vertraulichkeit der Kommunikation und globale Sicherheit. Die gerichtliche Überprüfung und die zunehmende Rechtsprechung zu diesen Fragen stehen im Mittelpunkt der Überlegungen zu diesem Thema.

Wie der allgemeine Bericht zeigt, besteht das Hauptproblem in diesem Bereich in der Gefahr einer Überregulierung in einem stark veränderlichen und unvorhersehbaren Bereich. Als solcher erfordert er gut koordinierte Regulierungsinstrumente, kann jedoch die wachsende Vielfalt der relevanten Aktivitäten nicht ignorieren. Aus institutioneller Sicht erscheint es jedoch wichtig, auf die Tendenz des Unionsgesetzgebers in allen oben genannten Bereichen hinzuweisen, als Harmonisierungsinstrument auf Regelungen zurückzugreifen, die den politischen Willen zur Annahme einheitlicher Regeln innerhalb der Europäischen Union zu veranschaulichen scheinen.

2. Besteuerung, staatliche Beihilfen und Wettbewerbsverzerrungen[8]

Nach der geltenden Rechtsprechung zu Steuerregelungen und staatlichen Beihilfen sind die Probleme der Steuervorbescheide und ihr Einfluss auf den Wettbewerb sowie das Ergebnis der Untersuchungen der Kommission und der laufenden oder künftigen Verfahren des Gerichtshofs von größter Bedeutung für die derzeitige Binnenmarktpolitik. In diesem Zusammenhang umfasst das vorliegende Thema die Beziehung zwischen Begriffen wie Gewinnverlagerung und schädlichem Steuerwettbewerb, Doppelbesteuerung und doppelter Nichtbesteuerung, einschließlich der OECD-Modellinstrumente. Es gibt auch einen Einblick in die territoriale Reichweite solcher Geschäfte und Abhilfemaßnahmen.

Wie der allgemeine Bericht zeigt, weisen sowohl die nationalen als auch die internationalen Steuersysteme nach wie vor Mängel auf, wobei in der Praxis die Steuerharmonisierung durch die Vorschriften über staatliche Beihilfen ersetzt wird. Das zunehmende Bewusstsein für die Rechtsprechung und die Learning-by-doing-Prozesse innerhalb der Kommission scheinen jedoch die Wirksamkeit der staatlichen Beihilferegelung zu verbessern. Angesichts der Tatsache, dass die Zukunft bedingungsloser Steuerausnahmen in der Europäischen Union in

[8] Generalberichterstatter: Professor Raymond Luja, Universität Maastricht (NL), Steuerberater von Loyens & Loeff N.V., Amsterdam (NL). Institutionelle Berichterstatterinnen: Frau Julia Rapp und Frau Ramona Ianus von der Europäischen Kommission.

Frage gestellt wird, sowie des Erfolgs der Rechtsvorschriften zur Bekämpfung der Steuervermeidung wird die Notwendigkeit von Steuervorbescheiden zunehmen. Aus institutioneller Sicht ist die Rolle der Kommission in dieser Hinsicht herausragend, aber sie kann nur auf der Grundlage von Leitlinien des Gerichtshofs der Europäischen Union angemessen umgesetzt werden.

3. Die externe Dimension der EU-Politiken: horizontale Aspekte; Handel und Investitionen; Einwanderung und Asyl[9]

Nicht zuletzt verdienen die externen Aspekte der europäischen Politik besondere Aufmerksamkeit. Die Entwicklung der internationalen Gemeinschaft in Zeiten politischer und militärischer Spannungen, die bereits zu erheblichen menschlichen und sozialen Kosten geführt haben mit dramatischer Auswirkung auf die künftige Politik der Europäischen Union, sollte dringend von angesehenen europäischen und internationalen Persönlichkeiten in Angriff genommen werden.

Vorab wird eine Aktualisierung der Verteilung von Zuständigkeiten und Befugnissen zwischen den EU-Organen und den Mitgliedstaaten und ihrer jeweiligen Rolle im internationalen Bereich gefordert. Dies würde eine eingehende und fokussierte Analyse zu einem Aspekt liefern, der im Rahmen des Themas III des XXVII. Kongresses in Budapest behandelt wurde. Zweitens konzentriert sich das Thema auf die internationalen Abkommen, die derzeit von der Europäischen Union über Handelsliberalisierung, Marktzugang und Investitionsschutz wie TTIP und CETA im Rahmen anderer regionaler oder globaler internationaler Abkommen ausgehandelt werden[10]. Vor dem Hintergrund der jüngsten Rechtsprechung des Gerichtshofs betrachtet der institutionelle Bericht

[9] Generalberichterstatter: Professorin Christine Kaddous, Universität Genf (CH), Gastprofessorin am Europakolleg (BL / PL) und an der Université Paris II Panthéon-Assas (FR); Professor Nuno Piçarra, Professor an der Rechtsfakultät der Universität Nova von Lissabon, Mitglied des Réseau académique d'études juridiques sur l'immigration et l'asile en Europe (*Odysseus*) und des Verwaltungsrates der Agentur der Europäischen Union für Grundrechte. Institutionelle Berichterstatter: Herr Hubert Légal und Herr Álvaro de Elera, Juristischer Dienst des Rates; Herr Freddy Drexler und Herr Anders Neergaard, Juristischer Dienst des Europäischen Parlaments.
Zum Zeitpunkt des Schreibens hatten die Berichterstatter keinen Zugang zu dem Urteil des Gerichtshofs in der Rechtssache C-284/16, *Slowakische Republik gegen Achmea BV*. In seinem Vorabentscheidungsverfahren vom 6. März 2018 kam der Gerichtshof zu dem Schluss, dass die Schiedsklausel im Abkommen zwischen den Niederlanden und der Slowakei (Intra-EU BIT) über den Investitionsschutz nicht mit dem Unionsrecht vereinbar ist. Das Urteil wirft weitere Fragen bezüglich der Schiedsgerichtsbarkeit in der Europäischen Union in der Investor-Staat-Streitbeilegung auf.

[10] Zum Zeitpunkt des Schreibens hatten die Berichterstatter keinen Zugang zu dem Urteil des Gerichtshofs in der Rechtssache C-284/16, *Slowakische Republik gegen Achmea BV*. In seinem Vorabentscheidungsverfahren vom 6. März 2018 kam der Gerichtshof zu dem Schluss, dass die Schiedsklausel im Abkommen zwischen den Niederlanden und der Slowakei (Intra-EU BIT) über den Investitionsschutz

gemischte Vereinbarungen als eine politische Entscheidung des Unionsgesetzgebers und wirft in diesem Zusammenhang die Frage nach den Bedingungen für den Rückgriff auf diese Art von Abkommen auf. In Bezug auf internationale Abkommen zeigt der Bericht auch die dringende Notwendigkeit, die Mechanismen der demokratischen Kontrolle innerhalb der Institutionen der Europäischen Union und der Mitgliedstaaten zu stärken.

Auf der anderen Seite bieten die immensen Herausforderungen der Einwanderung und des Asyls in unserem Raum der Freiheit, der Sicherheit und des Rechts die Gelegenheit zu einer intensiven Debatte. Es ist wichtig zu verstehen, wie sich die derzeitige Krise auf die bestehenden und sich entwickelnden Vorschriften, internationalen Abkommen, Praktiken und institutionellen Mechanismen auswirkt, die sich mit so grundlegenden Fragen wie dem Rechtsschutz und der Rechtsstaatlichkeit befassen. Wir sind der festen Überzeugung, dass die Europäische Union ein einzigartiger Rahmen ist, um all diese Ziele unter Wahrung der Grundrechte, der Demokratie und der Rechtsstaatlichkeit zu erreichen. Die Wahrung dieser Werte für die nächsten Generationen europäischer Bürger ist eines der wichtigsten Ziele unserer Zeit.

4. Weitere Debatten

Um einen breiteren Einblick in die Debatte zu geben, wurde ein einleitendes Podium über Europa am Scheideweg geplant. In ihren Eröffnungsvorträgen werden Professorin Catherine Barnard und Professor Michael O'Flaherty jeweils die „Zukunft Europas nach dem Brexit" und die „Grundrechte als Wegweiser am Scheideweg" diskutieren. Dieses Podium sollte einen hervorragenden Ausgangspunkt für die Debatte bieten, die von den prominenten Rednern des Podiums zu Europa und dem Brexit über eines der traumatischsten Ereignisse in der aktuellen Geschichte der Europäischen Union geführt wird.

IV. Worte der Dankbarkeit

Als Präsident und Vorstandsmitglieder der Portugiesische Gesellschaft für Europarecht (APDE – Associação Portuguesa de Direito Europeu) möchten wir Seiner Exzellenz, dem Präsidenten der Portugiesischen Republik, und Seiner Exzellenz, dem Premierminister Portugals, für die institutionelle Unterstützung des XXVIII. FIDE Kongresses danken, der vom 23. bis 26. Mai 2018 in Estoril von der APDE organisiert wurde.

Wir möchten auch allen Berichterstattern, Rednern, Vorsitzenden, Moderatoren und Dolmetschern danken, die zur Arbeit des Kongresses und dieser Veröffentlichung beigetragen haben.

nicht mit dem Unionsrecht vereinbar ist. Das Urteil wirft weitere Fragen bezüglich der Schiedsgerichtsbarkeit in der Europäischen Union in der Investor-Staat-Streitbeilegung auf.

Ohne den großzügigen Beitrag unserer Sponsoren und Unterstützer wäre die Organisation des XXVIII. FIDE Kongresses nicht möglich gewesen.

Die Unterstützung des Gerichtshofs der Europäischen Union und der Europäischen Kommission war ebenfalls von größter Bedeutung für den Erfolg des Kongresses.

Nicht zuletzt möchten wir insbesondere den Mitgliedern des Exekutivkomitees des Kongresses danken, Alberto Saavedra, Filipa Pimentel, Joana Schmid Moura, João de Lemos Portugal, Leonor Bettencourt Nunes, Margarida Rosado da Fonseca, Margarida Sameiro, Piedade Castro e Sousa und Teresa Côrte-Real. Ohne ihre bedingungslose Hingabe an den Kongress wäre die Organisation nicht möglich gewesen.

José Luís da Cruz Vilaça, Carlos Botelho Moniz, Nuno Piçarra, Rita Leandro Vasconcelos, João Paulo Teixeira de Matos, Nuno Ruiz, Miguel Gorjão-Henriques

QUESTIONNAIRE



QUESTIONNAIRE

Peggy Valcke*
Piedade Costa de Oliveira**

THEMES

1. Internal Market and electronic commerce : Internet and e-commerce

E-commerce and consumer protection: liability of internet intermediaries, consumer rights: geo-blocking; internet purchase and contractual rights; consumer protection and dispute resolution; sharing economy

E-Commerce Directive 2000/31/EC; Digital Consumer Rights proposals (on digital content and on digital contracts for goods)

2. Digital media

Distribution of audiovisual content over the Internet; Convergence with social media (free speech, hate speech); IP (possibly narrow to copyright) in the digital single market; AVMS Directive (under review); Copyright framework (under review)

3. Digital infrastructures

High-speed networks, spectrum management, net neutrality, Citizens and the internet: connection for all, web accessibility

* General rapporteur.
** Institutional rapporteur.

Electronic communications regulatory framework (under review), Web accessibility Directive

4. Data in the digital economy

'Data as an asset': free flow of data and the issue of data localisation. Emerging issues (arising mainly in the context of digitising industry and automation): open data, Machine-to-machine generated data (e.g. robots, automated cars): ownership, access and use; liability in case of harm

Citizen's fundamental rights (protection of personal data and privacy, especially in an increasingly digitised would (Internet of Things and Big Data; State security (surveillance)

General Data Protection Regulation – will enter into force May 2018, ePrivacy Directive, PNR Directive and PNR international agreements; adequacy decisions

TOPIC 1: INTERNAL MARKET AND DIGITAL ECONOMY

It is common ground that one of the most significant founding stones of the EU, namely the internal market, is heavily touched upon by the unprecedented changes brought by technological developments.

At EU level, in several areas of law existing legal instruments have recently been reviewed and new ones have been (or will be) added. All of them are intended to address new challenges brought by rapid technological developments and globalisation.

The Commission adopted the Digital Single Market Strategy in May 2015, setting out the major challenges and key actions it considered would need to be addressed.

Part of those actions were put forward in successive 'packages' from December 2015 onwards and may be grouped according to the three pillars identified in the Digital Single Market Strategy namely:

1) *Better access for consumers and businesses to online goods and services across Europe – this requires the rapid removal of key differences between the online and offline worlds to break down barriers to cross-border online activity.*
2) *Creating the right conditions for digital networks and services to flourish – this requires high-speed, secure and trustworthy infrastructures and content services, supported by the right regulatory conditions for innovation, investment, fair competition and a level playing field.*
3) *Maximising the growth potential of European Digital Economy – this requires investment in ICT infrastructures and technologies such as Cloud computing and Big Data, and research and innovation to boost industrial competiveness as well as better public services, inclusiveness and skills.*

The choice for the sub-topics of Topic 1 was guided not only by the fact that these are the ones on which courts are increasingly invited to decide on but also, and primarily, because those areas demonstrate the need to rethink legal concepts and to adapt the legal frameworks to new realities and challenges.

QUESTIONNAIRE

Internal market and digital economy

This questionnaire is intended to provide the framework for national and institutional reports on the sub-topics listed below.

1. Internal Market and electronic commerce : Internet and e-commerce

E-commerce and consumer protection: liability of internet intermediaries, consumer rights: geo-blocking; internet purchase and contractual rights; consumer protection and dispute resolution; sharing economy

E-Commerce Directive 2000/31/EC; Digital Consumer Rights proposals (on digital content and on digital contracts for goods)

1.1. Electronic Commerce, liability of Internet intermediaries

The E-Commerce Directive has created a regime of liability exemption for providers qualifying as 'mere conduit' and 'cache', combined with a notice-and-take-down procedure. This regime is not limited to intellectual property but extends to all kinds of responsibility issues, including criminal law. Liability issues and court injunctions have led to a series of decisions of the ECJ[1]. Thus, the 1st subtopic could raise the question of the systematic relevance of the concept of *intermediary* and the *liability exemption* attached thereto under the E-Commerce Directive.

[1] C-360/10 SABAM v Netlog NV, C-70/10 Scarlet Extended v. SABAM, C-324/09 L'Oréal a.o. v. eBay International AG a.o., Joined Cases C-236/08, C-237/08 and C-238/08 Google France and Google. Mc Fadden, Case C-484/14, 15.9.2016
C-160/15, Opinion of AG : §86. Although Article 14 of Directive 2000/31 seeks to restrict or exempt cases where intermediary information society service providers may be liable under national law, the exemptions in question are subject to strict conditions. In this regard, the Court ruled in paragraph 119 of the judgment in L'Oréal and Others (C-324/09, EU:C:2011:474) that a provider of hosting services (55) may, in situations in which that provider has confined itself to a merely technical and automatic processing of data, only be exempt, under Article 14(1) of Directive 2000/31, from any liability for unlawful data that it has stored 'on condition that it has not had "actual knowledge of illegal activity or information" and, as regards claims for damages, has not been "aware of facts or circumstances from which the illegal activity or information is apparent" or that, having obtained such knowledge or awareness, it has acted expeditiously to remove, or disable access to, the information'.

Q1.1.1: Which difficulties (e.g. definition, delimitation) were/are your Member State and national courts confronted with when laying down rules or deciding cases where the concept of intermediary service providers is at stake?

Q1.1.2: Do you think in L'Oréal v eBay, C-324/09, the CJEU has put forward a reasonable test for liability?

Q1.1.3: Is the regime of notice-and-take down appropriate in all kinds of situations (e.g. in cases of infringement of others' rights, such as intellectual property right, by costumers of ISSs; hate speech)?

If not, what could be other appropriate solutions?

Q1.1.4: Which difficulties were/are your Member State and national courts confronted with when considering injunctions?

(Scarlet v SABAM C-70/10+ SABAM v Netlog NV C-360/10: copyright filtering injunction would create a clash with other legal principles. However, the ECJ created a checklist for specific blocking requests)

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution[2]

Q1.2.1: Which difficulties were/are your Member State and national courts confronted with when considering remedies under the Consumer Sales and Guarantees Directive?

[2] Extract from SWD(2016)163 Guidance on UCPD
The UCPD only applies in B2C situations, the first step in assessing whether this Directive is applicable to any given online platform provider should be to evaluate whether it qualifies as a "trader" under Article 2(b) UCPD.
According to a case-by-case assessment, a platform provider may be acting for purposes relating to its business whenever, for example, it charges a commission on the transactions between suppliers and users, provides additional paid services or draws revenues from targeted advertising.
Furthermore, under Article 5(2) UCPD, no platform provider qualifying as a "trader" should act contrary to the requirements of professional diligence in its commercial practices towards consumers. Under Article 2(h) UCPD, 'professional diligence' means the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity.
The professional diligence duties of these traders vis-à-vis consumers under the UCPD is different from, whilst complementary to, the regime on exemptions from liability established under Article 14 of the e-Commerce Directive for illegal information hosted by service providers at the request of third parties. In particular, Article 14(1) is often invoked by some platforms, which argue that they merely act as intermediaries providing hosting services, as defined in that provision, and that they are thus not liable for the information stored. Furthermore, Article 15(1) of the e-Commerce Directive prevents Member States from imposing on such "hosting service providers" a general obligation to monitor the stored information or to actively engage in fact-finding.

Q1.2.2: Does the proposed Directive on certain aspects concerning contracts for the supply of digital content (COM(2015)634) provide for appropriate rules enabling the achievement of a genuine digital single market?

Q1.2.3: Does the proposed Directive on certain aspects concerning contracts for the online and other distance sales of goods (COM(2015)635) and the envisaged full harmonisation of key contractual rights provide for appropriate rules enabling the achievement of a genuine digital single market?

Q1.2.4: How do you evaluate the effect of the harmonised above rules on the enforcement of EU consumer protection legislation?[3]

Q1.2.5: Do you consider that current EU consumer protection law (i.e. Unfair Commercial Practices Directive 2005/29/EC; Unfair Contract Terms Directive 1993/13/EC and Directive 2011/83/EC on Consumer Rights) appropriate for protecting consumers in their dealings with online platforms?

Q1.2.6: Has there been any action before your national courts on the basis of consumer law against online providers' terms and conditions?

Q1.2.7: Do you consider it necessary/useful to expand the scope of the rules on Business to Consumers (B2C) to Business to Consumers (B2B)?

1.3. Geo-blocking

The Commission has presented a proposal on addressing unjustified geoblocking (COM(2016). The proposal defines specific situations when there can be no justified reasons for geo-blocking or other discriminations based on nationality, residence or location:

- when a customer buys a good, such as electronics, clothes, sportswear or a book, which the trader does not deliver cross-border;

[3] COM(2015)635, p. 7: *The full harmonisation approach has already proven successful in the area of EU consumer protection legislation, for instance through the rules of Directive 2011/83/EU, by ensuring a set of uniform consumer rights for all consumers within the European Union which are interpreted and enforced in a uniform way in all Member States. An initiative at EU level will secure the development of consumer rights in a coherent manner while ensuring that all consumers in the EU benefit from the same high level of consumer protection. It will create legal certainty for businesses which want to sell their goods in other Member States. Such a result can only be achieved by an action at the EU level.*
An initiative at EU level will secure the application of consumer rights in a coherent manner while ensuring that all consumers in the EU benefit from the same high level of consumer protection. It will create legal certainty for businesses which want to sell their goods in other Member States. Such an initiative will provide a consistent legal basis for coordinated enforcement actions as the proposed Directive will be included in the Annex of Regulation (EC) No 2006/2004 on cooperation of national authorities responsible for the enforcement of consumer protection laws. Moreover, enforcement actions would be largely facilitated by the proposed uniform fully harmonised rules.
Thus the enforcement of EU legislation will be strengthened for the benefit of EU consumers. Such a result can only be achieved by an action at the EU level.

- when a customer buys an electronically delivered service, such as cloud services, data warehousing, website hosting;
- when a customer buys a service which is supplied in the premises of the trader or in a physical location where the trader operates, such as a hotel room or a rental car. Furthermore, the proposal bans blocking of access to websites and the use of automatic rerouting if the customer has not given prior consent.

The proposal also provides for a non-discrimination rule in payments. While traders remain free to offer whatever payment means they want, the proposal includes a specific provision on non-discrimination within those payment means.

More information: https://ec.europa.eu/digital-single-market/en/geo-blocking-digitalsingle-market

Q1.3.1. The envisaged Regulation (COM(2016) aims at preventing unjustified discrimination on the basis of a consumer's domicile or nationality in cross-border situations. How do you see the interlink between this Regulation and Regulation 1215/2015 on the issue of a trader "directing activities to another Member State where the consumer has its domicile" for the purposes of determining jurisdiction?

1.4. Questions related to the collaborative economy (COM(2016)356)

Q1.4.1: What are the most contentious legal issues in your country raised by the collaborative economy businesses?

Q1.4.2: Competition issues: Does the fact that such businesses enter markets so far served by traditional service providers raise competition issues?

Q1.4.3: Market access requirements: What kind of service providers active in the collaborative economy required to obtain authorisations under national law in your country and under what conditions can such authorisations be obtained? Are the relevant administrative procedures and formalities clear and transparent?

Q1.4.4[4]: Consumer protection : Are consumer protection issues the subject of legal challenges in your country?

Q1.4.5: Under which conditions in a peer-to-peer provision of services the provider of the underlying service qualifies as a trader according to your national law?

[4] "EU consumer law applies to any collaborative platform that qualifies as a 'trader' and engages in 'commercial practices' vis-à-vis consumers. Conversely, EU consumer and marketing legislation does not apply to consumer-to-consumer transactions."

Q1.4.6: How can legal rules contribute to remedying the lack of consumer confidence in peerto-peer services? Do you think that trust-building mechanisms such as online rating and review systems and quality labels are appropriate tools to overcome the lack of information about individual service providers? What other tools would you consider appropriate?

2. Digital media

Distribution of audiovisual content over the Internet; Convergence with social media (free speech, hate speech); IP (possibly narrow to copyright) in the digital single market; AVMS Directive (under review); Copyright framework (under review); Portability of digital content

The media sector is undergoing a major transformation as a result of digitisation, the rise of the Internet and convergence between print and audiovisual media(*), as well as between traditional and social media.

These days we can watch our favourite programmes from all over Europe not just on TV, but also via the internet or on our mobile devices. Like other goods and services, the audiovisual media are subject to the rules of the single European market. The EU's Audiovisual Media Services Directive governs EU-wide coordination of national legislation on all audiovisual media, both traditional TV broadcasts and on-demand services. The AVMSD directive is currently open for review. A new legislative proposal amending the AVMSD has been adopted by the European Commission on 25 May 2016.

(*) Publishers of online newspapers and magazines increasingly offer clips on their websites as an add-on to written articles. Frequently, these clips are compiled in separate spaces of the websites with particular navigation tools for users (such as most recent videos, most watched videos), and they may cover the entire range of subjects reported on. The distinction between press products and audiovisual media services is crucial as different legal requirements and regulatory regimes apply. Publishers of newspapers, in printed form or online, are subject to a much lighter set of rules than audiovisual media services which are regulated by the EU Audiovisual Media Services Directive (AVMSD). Due to the convergence of media, the formerly distinct boundary between the two genres has become blurred. The Court of Justice of the European Union (CJEU) recently had to shed some light into how the exercise of classification of services may be carried out (New Media Online GmbH v Bundeskommunikationssenat; case C-347/14).

At the same time, and also in the context of its Digital Single Market Strategy, the Commission is rolling out an ambitious modernisation of the EU copyright framework. The objective is to make EU copyright rules fit for the digital age. The Commission published a Communication on a modern and more European copyright framework on 9 December 2015, together with a draft Regulation on

ensuring the cross-border portability of online content services in the internal market. This legislative initiative aims at ensuring that consumers who buy or subscribe to films, sport broadcasts, music, e-books and games can access them when they travel in other EU countries.

A second set of legislative proposals, adopted in September 2016, aims at modernising the copyright framework, focusing on allowing for wider online availability of content across the EU, adapting exceptions and limitations to the digital world, and achieving a well-functioning copyright market place. The package contains a draft Regulation which introduces the application of the country of origin to some online transmissions of broadcasting organisations, and the collective management of rights to retransmissions by means equivalent to cable (extending the specific regime for copyright licensing for TV and radio broadcasting by satellite and cable pursuant to Directive 93/83/EEC with a view to facilitating access to more television and radio programmes online from other EU countries).

More info: https://ec.europa.eu/digital-single-market/en/copyright

Q2.1: In its judgment of 21 October 2015 in *New Media Online GmbH v Bundeskommunikationssenat* (case C-347/14), the CJEU held that the concept of 'programme', within the meaning of Article 1(1)(b) of the AVMS Directive, must be interpreted as including, under the subdomain of a website of a newspaper, the provision of videos of short duration consisting of local news bulletins, sports and entertainment clips. It held that online newspapers are not per se excluded from the scope of the AVMSD. If publishers offer audiovisual material they may be covered by the Directive, provided that the principal purpose test is met.

Is your national practice in line with this judgment? If not, where does (or did) it deviate? Did the judgment of the CJEU lead to a different approach in your country?

Link to the judgment: http://curia.europa.eu/juris/liste.jsf?num=C-347/14 and the press release: http://curia.europa.eu/jcms/upload/docs/application/pdf/201510/cp150127en.pdf

Informative case note by the EBU: https://www.ebu.ch/files/live/sites/ebu/files/News/2015/10/Case%20note%20New%20 Media%20Online.pdf

Q2.2: The legislative proposal to amend the AVMS directive brings video platforms (such as YouTube) under the scope of the AVMS rules. Do you consider this a step in the right direction? How far should the extension of the scope of application towards such platforms go: only for the rules on protection of minors and the combatting of hate speech, or also for the rules on commercial communications (product placement, sponsoring, advertising...)? Does your national legislation already provide for sector-specific rules for audio-visual platforms?

Q2.3: One of the major areas of debate in the context of the AVMS revision, concerns the country-of-origin principle and the criteria for jurisdiction. Have there been any disputes in your country concerning the application of the country-of-origin principle (whereby the media regulator attempted to impose certain rules on audio-visual media service providers established in other Member States)? Have there been any problems regarding providers established outside the EU and targeting your national audience?

Q2.4: The AVMS Directive today does not impose any independence or other requirements for media regulators – in stark contrast with what is the case in e.g. the telecommunications or energy sector, or for data protection authorities. Would you consider the introduction of such independence requirements for media regulators at EU level a step forward? Would it facilitate the creation of a single market for audio-visual media services? Are there any national legal obstacles to such independence requirements for media regulators? Have there been any problems of undue political or commercial pressure on media regulators in your country?

Q2.5: What have been the most contentious issues in your country in relation to the application of broadcasting laws? (e.g. rules on commercial communications such as product placement or sponsoring? Unsuitable content for minors on television? The dissemination of hate speech? The role of public service broadcasters? Growing media concentration?) Do you think that some areas need further harmonisation through the AVMS Directive?

Q2.6: Have there been any initiatives in your country towards the offering of targeted (or addressable) advertising on television or of personalised content? If so, how was this dealt with under broadcasting/data protection laws? Was there any cooperation between the media regulator and the data protection authority? Do you see a need for an EU-wide harmonised approach?

Q2.7: Is the specific regime for copyright licensing for TV and radio broadcasting by satellite and cable (pursuant to Directive 93/83/EEC) still relevant in your country? Have similar rules been applied to online transmissions of broadcasting organisations?

Q2.8: What are the main barriers in your country to cross-border portability of digital content? Do you consider that the country of residence of the consumer should be controlled by the service provider on a regular basis? If yes, how to conciliate such requirement with the data minimisation principle under the GDPR?

3. Digital infrastructures

High-speed networks; spectrum management; net neutrality; Citizens and the internet: connection for all; web accessibility; electronic communications regulatory framework (under review); Web accessibility Directive

Telecommunications networks and services are the backbone of our information society. In recent decades, the EU has adopted a harmonised regulatory framework for electronic communications to improve competition, drive innovation, and boost consumer rights within the European single market. In 2015, it adopted rules on net neutrality (open internet) which it labelled as a "major achievement for the Digital Single Market". The rules in Regulation (EU) 2015/2120 prescribe that, in principle, all traffic has to be treated equally, and that every European must be able to have access to the open internet and that all content and service providers must be able to provide their services via a high-quality open internet. Under these rules, blocking, throttling and discrimination of internet traffic by Internet Service Providers (ISPs) is not allowed in the EU, save for three exhaustive exceptions (compliance with legal obligations; integrity of the network; congestion management in exceptional and temporary situations) and users are free to use their favourite apps and services no matter the offer they subscribe to.

The EU also launched several initiatives to promote investment in broadband networks supporting high-speed Internet. In September 2016, in the light of its Digital Single Market strategy, the Commission adopted a set of measures – the so-called "connectivity package" – to place the EU at the forefront of internet connectivity and achieve a European "Gigabit Society", including a proposal for a new European Electronic Communications Code. The Code further stimulates competition, and strengthens the internal market as well as consumer rights and wants more forward-looking and simplified rules that make it more attractive for all companies to invest in new top-quality infrastructures in the EU.

Q3.1: Did your country have rules on net neutrality in place before the adoption of Regulation (EU) 2015/2120? If so, were they more or less strict in comparison to the Regulation? What is the national approach towards practices of zero-rating (which are not explicitly prohibited by the Regulation)?

Q3.2: Should the EU go further in creating a single market for telecommunications networks or services (and introduce e.g. an EU-wide licensing scheme)? Did your national authorities adopt any special broadband measures and were they the result of EU intervention or adopted at own initiative?

Q3.3: Are there legal issues on spectrum management in your country? If yes, how have them been solved?

Q3.4: Have questions linked with the independence of NRAs been raised in your country? If yes, did they lead to legal challenges? How have they been solved?

4. Data in the digital economy

'Data as an asset': free flow of data and the issue of data localisation. Emerging issues (arising mainly in the context of digitising industry and automation): open data, Machine-to-machine generated data (e.g. robots, automated cars): ownership, access and use; liability in case of harm

Citizen's fundamental rights (protection of personal data and privacy, especially in an increasingly digitised would (Internet of Things and Big Data; State security (surveillance)

General Data Protection Regulation – will enter into force May 2018, ePrivacy Directive, PNR Directive and PNR international agreements; adequacy decisions.

Q4.1: How is your country preparing for the entry into force of the General Data Protection Regulation in May 2018? Are there any specific legislative proposals or executive measures in preparation?

Q4.2: How are businesses in your country adapting to the new requirements of the GDPR such as those related to consent, impact assessments, privacy by design and by default?

Q4.3: What are the most contentious issues in your country (from a legal viewpoint) in relation to IoT (Internet of Things) / smart cities / Machine-to-machine generated data / automated cars? (Ownership issues? Access and use? Liability in case of harm?) Are there any specific legislative measures or regulatory opinions/decisions in this area? What is the status of the policy debate?

Q4.4: Since the CJEU's controversial judgment in May 2014 in the Google Spain (or Costeja) case, the so-called "right to be forgotten" (or to be delisted) has received a lot of attention in Europe and beyond. What is the legal status in your country? Are complaints being brought before the data protection authority and/or courts? Has there been a growing body of case law in this regard? How is the balance struck between the individual's right to data protection and the other interests at stake (in particular the search engine's commercial freedom, the public's right to information and the author's right to free expression)?

QUESTIONNAIRE

Peggy Valcke*
Piedade Costa de Oliveira**

SUJETS

1. Marché Intérieur et commerce électronique: Internet et commerce électronique

Commerce électronique et protection des consommateurs: responsabilité des intermédiaires de l'Internet, droits des consommateurs: blocage géographique; achat sur Internet et droits contractuels; protection des consommateurs et résolution de litiges; économie du partage

Directive 2000/31/CE sur le commerce électronique; propositions en matière de droits des consommateurs dans l'environnement digital (concernant les contenus numériques et les contrats numériques portant sur des biens)

2. Médias numériques

Distribution de contenus audiovisuels sur Internet; Convergence avec les médias sociaux (liberté d'expression, discours de haine); PI (éventuellement restreindre au droit d'auteur) dans le marché unique numérique; Directive SMAV (en cours de révision); Cadre du droit d'auteur (en cours de révision)

* Rapporteur général.
** Rapporteur institutionnel.

3. Infrastructures numériques

Réseaux à haut débit, gestion du spectre, neutralité de l'Internet, Citoyens et l'Internet: connexion pour tous, accessibilité du Web

Cadre réglementaire des communications électroniques (en cours de révision), directive de l'accessibilité du Web.

4. Données dans l'économie numérique

'Les données comme un actif': libre circulation des données et la question de la localisation des données. Questions émergentes (qui se posent principalement dans le contexte de la numérisation de l'industrie et de l'automatisation): données ouvertes, données générées machine à machine (par exemple, robots, voitures automatisées): propriété, accès et utilisation; responsabilité en cas de préjudice

Les droits fondamentaux des citoyens (protection des données personnelles et de la vie privée, surtout dans un monde de plus en plus numérisé (l'Internet des Objets et les mégadonnées («Big Data»); sûreté de l'État (surveillance)

Règlement général sur la protection des données – entrera en vigueur en mai 2018, directive «Vie privée et communications électroniques», directive PNR et accords internationaux PNR; décisions en matière d'adéquation

THÈME 1 : LE MARCHÉ INTÉRIEUR ET L'ÉCONOMIE DIGITALE

Il est constant que l'une des plus importantes pierres fondatrices de l'Union européenne, à savoir le marché intérieur, est fortement touché par les changements sans précédent apportés par les développements technologiques.

Au niveau d'l'UE, dans plusieurs domaines du droit les instruments juridiques existants ont récemment été revus et des nouveaux ont été (ou seront) ajoutés. Tous visent faire face aux nouveaux défis apportés par les rapides développements technologiques et par la mondialisation.

La Commission a adopté la stratégie pour un marché unique numérique en mai 2015, énonçant les principaux défis et actions clés qu'elle a considérés comme devant être pris en charge. Une partie de ces actions a été présentée dans des 'paquets' successifs depuis décembre, ces actions pouvant être regroupées suivant les trois piliers identifiés dans la stratégie pour un marché unique numérique, à savoir :

1) *Améliorer l'accès des consommateurs et des entreprises aux produits et services en ligne dans l'ensemble de l'Europe – ce qui requiert de supprimer rapidement les principales différences entre les mondes en ligne et hors ligne afin d'éliminer les obstacles à l'activité transfrontalière en ligne.*

2) *Créer des conditions propices au développement des réseaux et des services numériques – ce qui requiert des infrastructures et des services de contenus haut débit, sécurisés et fiables, soutenus par des conditions réglementaires propices à l'innovation, à l'investissement, à la concurrence loyale et à des conditions équitables.*
3) *Maximiser le potentiel de croissance de l'économie numérique européenne – ce qui requiert des investissements dans les infrastructures TIC et dans des technologies telles que l'informatique en nuage («Cloud computing») et les mégadonnées («Big Data»), et la recherche et l'innovation pour stimuler la compétitivité industrielle ainsi que l'amélioration des services publics, de l'inclusion et des compétences.*

Le choix des sous-thèmes du Thème 1 a reposé non seulement sur le fait que ce sont ceux sur lesquels les tribunaux sont de plus en plus invités à se prononcer mais aussi, et surtout, parce que ces domaines démontrent la nécessité de repenser les concepts juridiques et d'adapter les cadres juridiques aux nouvelles réalités et aux nouveaux défis.

QUESTIONNAIRE

Le marché intérieur et l'économie digitale

Ce questionnaire est destiné à fournir le cadre pour les rapports nationaux et institutionnels sur les sous-thèmes énumérés ci-dessous.

1. Marché Intérieur et commerce électronique: Internet et commerce électronique

Commerce électronique et protection des consommateurs: responsabilité des intermédiaires de l'Internet, droits des consommateurs: blocage géographique; achats sur Internet et droits contractuels; protection des consommateurs et résolution de litiges; économie du partage

Directive 2000/31/CE sur le commerce électronique; propositions en matière de droits des consommateurs dans l'environnement digital (concernant les contenus numériques et les contrats numériques portant sur des biens)

1.1. Commerce électronique, responsabilité des intermédiaires de l'Internet

La directive sur le commerce électronique a créé un régime d'exonération de la responsabilité des prestataires lorsqu'ils sont considérés comme opérant un « simple transport » et une forme de stockage dite « caching », en combinaison avec une procédure de notification et de retrait. Ce régime n'est pas limité à la propriété intellectuelle, mais s'étend à tous types de questions de responsabi-

lité, y compris de droit pénal. Des questions de responsabilité et des injonctions des tribunaux ont conduit à une série de décisions de la CJCE[1]. Ainsi, le 1er sous-thème pourrait soulever la question de la pertinence systématique de la notion d'*intermédiaire* et l'*exemption de responsabilité* qui y est attachée dans le cadre de la directive sur le commerce électronique.

Q1.1.1: À quelles difficultés (par exemple, définition, délimitation) votre État membre et vos tribunaux nationaux se sont ils retrouvés/se retrouvent-ils confrontés lorsqu'ils fixent des règles ou décident des cas où le concept de prestataires de services intermédiaires est en jeu?

Q1.1.2 : Pensez-vous que dans l'affaire L'Oréal c/ eBay, C-324/09, la CJUE a présenté un critère raisonnable de responsabilité?

Q1.1.3: Le régime de notification et de retrait est-il approprié dans tous les types de situations (p. ex., dans les cas de violation des droits d'autrui, comme le droit de propriété intellectuelle, par des clients d'ISSs; discours de haine)?

Dans la négative, quelles pourraient être d'autres solutions appropriées?

Q1.1.4: À quelles difficultés votre État membre et vos tribunaux nationaux se sont-ils retrouvés/se retrouvent-ils confrontés lorsqu'ils considèrent des injonctions?

(Scarlet c/ SABAM C-70/10 + SABAM c/ Netlog NV C-360/10: l'injonction de filtrage de droit d'auteur susciterait un conflit avec d'autres principes juridiques. Toutefois, la CJCE a créé une liste de contrôle pour des demandes de blocage spécifiques)

[1] C-360/10 SABAM c/ Netlog NV, C-70/10 Scarlet Extended c/ SABAM, C-324/09 L'Oréal e.a. c/ eBay International AG e.a., affaires jointes C-236/08, C-237/08 et C-238/08 Google France et Google.
Mc Fadden, affaire C-484/14, 15.09.2016
C-160/15, conclusions de l'avocat général: §86. Bien que l'article 14 de la directive 2000/31 vise à restreindre ou à exempter des cas où les prestataires intermédiaires de services de la société d'information peuvent être tenus responsables en vertu du droit national, les dérogations en cause sont soumises à des conditions strictes. À cet égard, la Cour a jugé au point 119 de l'arrêt L'Oréal et autres (C-324/09, UE:C:2011:474) que le prestataire de services d'hébergement (55) peut, dans les situations où ce prestataire s'est limité à un traitement purement technique et automatique des données, être exonéré, en vertu de l'article 14, paragraphe 1, de la directive 2000/31, de toute responsabilité pour les données à caractere illégal qu'il a stockées que «à la condition qu'il n'ait pas eu "effectivement connaissance de l'activité ou de l'information illégale" et, en ce qui concerne les demandes en dommages et intérêts, qu'il n'ait pas eu "connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illégale est apparente" ou que, après avoir acquis une telle connaissance ou conscience, il ait promptement agi pour retirer les données en cause ou rendre l'accès à celles-ci impossible'.

1.2. Protection des consommateurs en matière d'Internet et de commerce électronique, d'achats sur internet et de droits contractuels ; protection des consommateurs et résolution de litiges [2]

Q1.2.1: À quelles difficultés votre État membre et vos tribunaux nationaux se sont-ils retrouvés/se retrouvent-ils confrontés lors de l'appréciation des recours dans le cadre de la directive sur certains aspects de la vente et des garanties des biens de consommation?

Q1.2.2: La directive proposée concernant certains aspects des contrats de fourniture de contenu numérique (COM(2015)634) prévoit-elle des règles appropriées permettant la mise en place d'un véritable marché unique numérique?

Q1.2.3: La directive proposée concernant certains aspects des contrats de ventes en ligne et de toute autre vente à distance de biens (COM(2015)635) et l'harmonisation complète de certains droits contractuels essentiels prévoit-elle des règles appropriées permettant la mise en place d'un véritable marché unique numérique?

[2] Extrait du document de travail des services de la Commission [SWD](2016)163 Orientations concernant la DPCD [Directive relative aux pratiques commerciales deloyales]
La DPCD s'appliquant qu'aux situations où des entreprises s'adressent aux consommateurs, la première étape pour apprécier si cette directive est applicable au prestataire d'une plate-forme en ligne donnée, consiste à évaluer s'il a la qualité de « professionnel » aux termes de l'article 2, point b), de la DPCD.
Dans le cadre d'une évaluation au cas par cas, un prestataire de plate-forme peut agir à des fins qui entrent dans le cadre de son activité commerciale dès lors, par exemple, qu'il facture une commission sur les transactions entre fournisseurs et utilisateurs, fournit des services supplémentaires payants ou tire des recettes de publicités ciblées.
En outre, au titre de l'article 5, paragraphe 2, de la DPCD, aucun prestataire de plate-forme ayant qualité de «professionnel» ne devrait contrevenir aux exigences de la diligence professionnelle dans ses pratiques commerciales vis-à-vis du consommateur. Au titre de l'article 2, point h), de la DPCD, on entend par "diligence professionnelle" le niveau de compétence spécialisée et de soins dont le professionnel est raisonnablement censé faire preuve vis-à-vis du consommateur, conformément aux pratiques de marchés honnêtes et/ou au principe général de la bonne foi dans son domaine d'activité.
Les obligations de diligence professionnelle vis-à-vis des consommateurs imposées à ces professionnels par la DPCD se distinguent, tout en le complétant, du régime d'exemption de responsabilité établi par l'article 14 de la directive sur le commerce électronique pour les informations illicites hébergées par des prestataires de service à la demande de tierces parties.
En particulier, l'article 14, paragraphe 1, est souvent invoqué par certaines plates-formes qui affirment agir en tant que simples intermédiaires fournissant des services d'hébergement tels qu'ils sont définis dans cette disposition, et qui n'assument donc pas la responsabilité des informations stockées.
En outre, l'article 15, paragraphe 1, de la directive sur le commerce électronique interdit aux États membres d'imposer à de tels «prestataires de service d'hébergement» une obligation générale de surveillance des informations qu'ils stockent ou de recherche active de faits.

Q1.2.4: Comment évaluez-vous l'effet des règles harmonisées ci-dessus relatives à l'application de la législation de l'UE en matière de protection des consommateurs?[3]

Q1.2.5: Considérez-vous que l'actuelle législation de l'UE en matière de protection des consommateurs (c.-à-d. la directive 2005/29/CE sur les pratiques commerciales déloyales; la directive 1993/13/CEE du Conseil concernant les clauses abusives dans les contrats conclus avec les consommateurs et la directive 2011/83/UE relative aux droits des consommateurs) est appropriée pour protéger les consommateurs dans leurs relations avec les plateformes en ligne?

Q1.2.6: Des actions basées sur la législation en matière de protection des consommateurs contre des «termes et conditions» de fournisseurs de services en ligne ont-elles été portées devant vos tribunaux?

Q1.2.7: Cela vous paraît-il nécessaire/utile d'étendre le champ d'application des règles concernant les relations entre entreprises et consommateurs (B2C) aux relations entre entreprises (B2B)?

1.3. Blocage géographique

La Commission a présenté une proposition visant régler le blocage géographie injustifié (COM(2016). La proposition définit certaines situations spécifiques dans lesquelles le blocage géographique ou autres discriminations fondées sur la nationalité, le lieu de résidence ou le lieu d'établissement, ne sauraient se justifier:

- lorsqu'un client achète une marchandise, telle que des produits électroniques, des vêtements, des vêtements de sport ou un livre, dont la livraison à l'étranger n'est pas assurée par le professionnel;

[3] COM(2015)635, p. 7: L'approche de l'harmonisation complète a déjà fait ses preuves dans le domaine de la législation de l'UE en matière de protection des consommateurs, dans le cadre des règles de la directive 2011/83/UE par exemple, en garantissant à tous les consommateurs de l'Union européenne un ensemble de droits uniformes, interprétés et appliqués de manière identique dans tous les États membres. Une initiative au niveau de l'UE garantira le développement cohérent des droits des consommateurs, tout en faisant en sorte que l'ensemble des consommateurs de l'UE bénéficient du même niveau élevé de protection. Elle sera source de sécurité juridique pour les entreprises qui souhaitent vendre leurs produits dans d'autres États membres. Un tel résultat ne peut être atteint que par une action au niveau de l'UE. *Une initiative au niveau de l'UE garantira l'instauration cohérente de droits pour les consommateurs, tout en offrant à l'ensemble des consommateurs de l'UE le même niveau élevé de protection. Elle sera source de sécurité juridique pour les entreprises qui souhaitent vendre leurs produits dans d'autres États membres. L'initiative fournira une base juridique cohérente pour la coordination des mesures de contrôle de l'application de la réglementation, étant donné que la directive proposée sera mentionnée à l'annexe du règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs. En outre, ces mesures de contrôle de l'application de la réglementation seraient largement facilitées par les règles pleinement harmonisées et uniformes proposées. Ainsi, le contrôle de l'application de la législation de l'UE sera renforcé au profit des consommateurs de l'UE. Un tel résultat ne peut être atteint que par une action au niveau de l'UE.*

- lorsqu'un client achète un service fourni par voie électronique, tel que des services d'informatique en nuage, des services de stockage de données, hébergement de sites;
- lorsqu'un client achète un service qui est fourni dans les locaux du professionnel ou dans un endroit où le professionnel exerce son activité, comme une chambre d'hôtel ou une voiture de location.

En outre, la proposition interdit le blocage de l'accès aux sites Web et l'utilisation du réacheminement automatique lorsque le client n'a pas donné son consentement préalable. La proposition prévoit également une règle de non-discrimination par rapport aux paiements. Alors que les professionnels restent libres d'offrir tous les moyens de paiement qu'ils veulent, la proposition contient une disposition spécifique sur la non-discrimination au sein de ces moyens de paiement.

Plus d'informations: https://ec.europa.eu/digital-single-market/en/geo-blocking-digitalsingle-market

Q1.3.1. Le règlement envisagé (COM(2016) vise à empêcher la discrimination injustifiée fondée sur le lieu de résidence du consommateur ou la nationalité dans des situations transfrontalières. Comment voyez-vous l'interaction entre ce règlement et le règlement 1215/2015 sur la question d'un professionnel qui « dirige des activités vers un autre État membre où le consommateur a son domicile» aux fins de déterminer la compétence?

1.4. Questions liées à l'économie collaborative (COM (2016)356)

Q1.4.1: Quelles sont les questions juridiques les plus controversées dans votre pays, soulevées par les entreprises de l'économie collaborative?

Q1.4.2: Questions de concurrence: Est-ce que le fait que ces entreprises s'implantent dans des marchés jusqu'à présent desservis par des prestataires de services traditionnels soulève des questions de concurrence?

Q1.4.3: Conditions d'accès au marché: Quels types de prestataires de services actifs dans l'économie collaborative ont cherché à obtenir des autorisations conformément à la loi nationale dans votre pays et dans quelles conditions de telles autorisations peuvent-elles être obtenues? Les procédures administratives et les formalités pertinentes sont-elles claires et transparentes?

Q1.4.4: Protection des consommateurs[4]: Est-ce que des questions en matière de protection des consommateurs font l'objet de contestations en justice dans votre pays?

[4] "La législation de l'UE en matière de protection des consommateurs s'applique à toute plateforme collaborative qui a la qualité de 'professionnel' et qui recourt à des 'pratiques commerciales' vis-à-vis de

Q1.4.5: Dans quelles conditions, dans une prestation de services entre pairs, le prestataire du service sous-jacent assume-t-il la qualité de professionnel selon votre droit national?

Q1.4.6: Comment les règles juridiques peuvent-elles contribuer à remédier au manque de confiance des consommateurs dans les services pair à pair? Pensez-vous que les mécanismes visant à renforcer la confiance tels que les systèmes de classement et d'évaluation en ligne et les labels de qualité sont des outils adéquats pour remédier au manque d'informations sur les différents prestataires de services? Quels autres outils considéreriez-vous comme appropriés?

2. Médias numériques

Distribution de contenus audiovisuels sur Internet; Convergence avec les médias sociaux (liberté d'expression, discours de haine); PI (éventuellement restreindre au droit d'auteur) dans le marché unique numérique; Directive SMAV (en cours de révision); Cadre du droit d'auteur (en cours de révision); Portabilité de contenus numériques

Le secteur des médias est en train de subir une transformation majeure en raison de la numérisation, de l'essor de l'Internet et la convergence entre les médias imprimés et audiovisuels(*), ainsi qu'entre médias traditionnels et sociaux.

De nos jours, nous pouvons regarder nos émissions préférées provenant de toute l'Europe non seulement à la télévision, mais aussi via Internet ou sur nos appareils mobiles. Comme les autres biens et services, les médias audiovisuels sont soumis aux règles du marché unique européen. La directive «Services de médias audiovisuels» de l'UE régit la coordination à l'échelle de l'UE des législations nationales relatives à tous les médias audiovisuels, tant la radiodiffusion télévisuelle traditionnelle comme les services à la demande. La directive SMAV fait actuellement l'objet de révision. Une nouvelle proposition législative modifiant la directive SMAV a été adoptée par la Commission européenne le 25 mai 2016.

(*) Les éditeurs de magazines et de journaux en ligne offrent de plus en plus de clips sur leurs sites en tant que complément aux articles écrits. Fréquemment, ces clips sont compilés dans des espaces séparés des sites web avec des outils de navigation particulière pour les utilisateurs (tels que les plus récentes vidéos, les vidéos les plus regardées), et ils peuvent couvrir toute la gamme de sujets rapportés. La distinction entre produits de la presse et les services de médias audiovisuels est cruciale étant donné que différentes exigences juridiques et différents régimes réglementaires s'appliquent. Les éditeurs de journaux, sous forme imprimée ou en ligne, sont soumis à un ensemble de règles beaucoup plus léger que les services de

consommateurs. La législation de l'UE en matière de protection des consommateurs et de commercialisation ne s'applique pas par contre aux transactions de consommateur à consommateur."

médias audiovisuels qui sont réglementés par la directive «Services de médias audiovisuels» (SMAV) de l'UE. En raison de la convergence des médias, la frontière autrefois distincte entre les deux genres s'est estompée. La Cour de Justice de l'Union européenne (CJUE) a récemment dû éclaircir la manière dont l'exercice de classification des services peut-être être effectué (New Media Online GmbH c/ Bundeskommunikationssenat; affaire C-347/14).

En même temps, et aussi dans le cadre de sa stratégie pour un marché unique numérique, la Commission est en train de lancer une ambitieuse modernisation du cadre de l'UE en matière de droit d'auteur. L'objectif est d'adapter les règles de l'UE en matière de droit d'auteur à l'ère numérique. La Commission a publié une communication relative à un cadre moderne et plus européen pour le droit d'auteur le 9 décembre 2015, ainsi qu'un projet de règlement visant à assurer la portabilité transfrontière des services de contenu en ligne dans le marché intérieur. Cette initiative législative vise à garantir que les consommateurs qui achètent ou souscrivent des films, émissions de sport, musiques, livres numériques et jeux peuvent y accéder lorsqu'ils voyagent dans d'autres pays de l'UE.

Une deuxième série de propositions législatives, adoptées en septembre 2016, vise à moderniser le cadre du droit d'auteur, en mettant l'accent sur permettre une plus grande disponibilité de contenus en ligne dans toute l'UE, adapter les exceptions et limitations au monde numérique et mettre en place un marché de droit d'auteur performant. Le paquet contient un projet de règlement qui introduit la demande du pays d'origine à certaines transmissions en ligne d'organismes de radiodiffusion, et la gestion collective des droits de retransmission par des moyens équivalents au câble (étendant le régime spécifique des licences de droit d'auteur pour la radiodiffusion télévisuelle et radiophonique par satellite et par câble conformément à la directive 93/83/CEE en vue de faciliter l'accès à davantage d'émissions de radio et de télévision en ligne en provenance d'autres pays de l'UE).

Plus d'informations: https://ec.europa.eu/digital-single-market/en/copyright

Q2.1: Dans son arrêt du 21 octobre 2015 dans *New Media Online GmbH c/ Bundeskommunikationssenat* (affaire C-347/14), la CJUE a considéré que la notion de 'programme', au sens de l'article 1er, paragraphe 1, point b), de la Directive SMAV, doit être interprétée en ce sens qu'elle comprend la mise à disposition, sur un sousdomaine du site Internet d'un journal, de vidéos de courte durée qui correspondent à de courtes séquences extraites de bulletins d'informations locales, de sport ou de divertissement. La Cour a considéré que les journaux en ligne ne sont pas automatiquement exclus du champ d'application de la directive SMAV. Si les éditeurs offrent des éléments audiovisuels, ils peuvent être couverts par la directive, pourvu que le critère de l'objet principal soit rempli. Votre pratique nationale est-elle conforme à cet arrêt? Dans la négative, en quoi est-ce qu'elle en dévie (ou en déviait)? L'arrêt de la CJUE a-t-il conduit à une approche différente dans votre pays ?

Lien vers l'arrêt: http://curia.europa.eu/juris/liste.jsf?num=C-347/14 et vers le communiqué de presse: http://curia.europa.eu/jcms/upload/docs/application/pdf/201510/cp150127en.pdf

Note informative sur le cas par l'UER : https://www.ebu.ch/files/live/sites/ebu/files/News/2015/10/Case%20note%20New%20 Media%20Online.pdf

Q2.2: La proposition législative en vue de modifier la directive SMAV place les plateformes vidéo (telles que YouTube) dans le champ d'application des règles SMAV. Considérez-vous cela comme un pas dans la bonne direction? Jusqu'où doit aller l'extension du champ d'application à ces plateformes: seulement jusqu'aux règles sur la protection des mineurs et la lutte contre les discours de haine, ou également jusqu'aux règles sur les communications commerciales (placements de produits, parrainage, publicité...)? Votre législation nationale prévoit-elle déjà des règles sectorielles pour les plateformes audiovisuelles?

Q2.3: L'un des principaux domaines de débat dans le cadre de la révision de la SMAV, porte sur le principe du pays d'origine et les critères pour déterminer la compétence. Y a-t-il eu des litiges dans votre pays concernant l'application du principe du pays d'origine (dans lesquels le régulateur des médias a tenté d'imposer certaines règles aux prestataires de services de médias audiovisuels établis dans d'autres États membres)? Y a-t-il eu des problèmes concernant des prestataires établis en dehors de l'UE et ciblant votre audience nationale?

Q2.4: La directive SMAV n'impose aujourd'hui aucune exigence d'indépendance ou autres aux régulateurs des médias – en net contraste avec ce qu'il se passe, par exemple, dans le secteur des télécommunications ou de l'énergie, ou relativement aux autorités chargées de la protection des données. Considéreriez-vous l'introduction de ces exigences d'indépendance relativement aux régulateurs des médias au niveau de l'UE un pas en avant? Cela faciliteraitil la création d'un marché unique pour les services de médias audiovisuels? Y a-t-il des obstacles juridiques nationaux à ces exigences d'indépendance pour les régulateurs des médias? Y a-t-il eu des problèmes de pression politique ou commerciale indue sur les régulateurs des médias dans votre pays?

Q2.5: Quelles ont été les questions les plus controversées dans votre pays en ce qui concerne l'application des lois de radiodiffusion? (par exemple, les règles sur les communications commerciales telles que le placement de produit ou le parrainage? Contenus inappropriés pour les mineurs à la télévision? La diffusion de discours de haine? Le rôle des radiodiffuseurs de service public? Concentration croissante des médias?) Pensez-vous que certains domaines ont besoin d'une plus grande harmonisation par le biais de la directive SMAV?

Q2.6: Y a-t-il eu des initiatives dans votre pays en matière de publicité ciblée (ou adressable) à la télévision ou de contenu personnalisé? Dans l'affirmative, comment cela a-t-il été traité dans le cadre des lois relatives à la radiodiffusion

/à la protection des données? Y a-t-il eu une coopération entre le régulateur des médias et l'autorité chargée de la protection des données? Voyez-vous la nécessité d'une approche harmonisée à l'échelle de l'UE?

Q2.7: Le régime spécifique d'octroi de licences de droit d'auteur pour la radiodiffusion télévisuelle et sonore par satellite et par câble (conformément à la directive 93/83/CEE du Conseil) est-il toujours pertinent dans votre pays? Des règles similaires ont-elles été appliquées aux transmissions en ligne des organismes de radiodiffusion?

Q2.8: Quels sont les principaux obstacles dans votre pays concernant la portabilité transfrontalière des contenus numériques? Considérez-vous que le pays de résidence du consommateur doive être régulièrement contrôlé par le prestataire de services? Dans l'affirmative, comment concilier cette exigence avec le principe de minimisation des données sous le RGPD?

3. Infrastructures numériques

Réseaux à haut débit, gestion du spectre, neutralité de l'Internet, Citoyens et l'Internet: connexion pour tous, accessibilité du Web

Cadre réglementaire des communications électroniques (en cours de révision), directive de l'accessibilité du Web

Les réseaux et services de télécommunications sont la colonne vertébrale de notre société de l'information. Au cours des dernières décennies, l'UE a adopté un cadre réglementaire harmonisé pour les communications électroniques afin d'améliorer la concurrence, d'encourager l'innovation, et de renforcer les droits des consommateurs au sein du marché unique européen. En 2015, elle a adopté des règles sur la neutralité de l'Internet (Internet ouvert) qu'elle a qualifié de «réalisation majeure pour le marché unique numérique». Les règles du règlement (UE) 2015/2120 prescrivent que, en principe, tout le trafic doit être traité de manière égale, et que tous les Européens doivent être en mesure d'avoir accès à l'Internet ouvert et que tous les fournisseurs de contenus et de services doivent être en mesure de fournir leurs services via un internet ouvert de haute qualité. En vertu de ces règles, le blocage, les limitations et la discrimination du trafic Internet par les fournisseurs de services Internet (FSI) ne sont pas autorisés dans l'UE, sauf trois exceptions exhaustives (le respect d'obligations légales; l'intégrité du réseau; la gestion de la congestion dans des situations exceptionnelles et temporaires) et les utilisateurs sont libres d'utiliser leurs applications et services préférés, peu importe l'offre à laquelle ils souscrivent.

L'UE a également lancé plusieurs initiatives visant à promouvoir l'investissement dans les réseaux à large bande qui soutiennent l'Internet haut débit. En Septembre 2016, à la lumière de sa stratégie pour un marché unique numérique ,

la Commission a adopté un ensemble de mesures – le «paquet de connectivité» – de façon à placer l'UE à la pointe de la connectivité Internet et de mettre en place une «société gigabit» européenne, incluant une proposition pour un nouveau code européen des communications électroniques. Le Code stimule davantage la concurrence, et renforce le marché intérieur, ainsi que les droits des consommateurs et prévoit des règles tournées vers l'avenir et simplifiées qui favorisent l'investissement de toutes les entreprises dans de nouvelles infrastructures de haute qualité dans l'UE.

Q3.1: Votre pays avait-il des règles sur la neutralité de l'Internet établies avant l'adoption du règlement (UE) 2015/2120? Dans l'affirmative, étaient-elles plus ou moins strictes par rapport au règlement? Quelle est l'approche nationale en ce qui concerne les pratiques de «fixation de taux zéro» (qui ne sont pas expressément interdites par le règlement)?

Q3.2: L'UE devrait-elle aller plus loin dans la création d'un marché unique pour les réseaux ou services de télécommunications (et introduire, par exemple, un système d'octroi de licences à l'échelle de l'UE)? Vos autorités nationales ont-elles adopté des mesures spéciales de bande large et ont-elles été le résultat d'une intervention de l'UE ou ont-elles été adoptées de leur propre initiative?

Q3.3. Des questions juridiques sont-elles soulevées dans votre pays en ce qui concerne la gestion du spectre? Dans l'affirmative, comment ont-elles été résolues?

Q3.4. Des questions liées à l'indépendance des ARN ont-elles été soulevées dans votre pays? Dans l'affirmative, ont-elles conduit à des contestations en justice? Comment ont-elles été résolues?

4. Données dans l'économie numérique

'Les données comme un actif': libre circulation des données et la question de la localisation des données. Questions émergentes (qui se posent principalement dans le contexte de la numérisation de l'industrie et de l'automatisation): données ouvertes, données générées machine à machine (par exemple, robots, voitures automatisées): propriété, accès et utilisation; responsabilité en cas de préjudice

Les droits fondamentaux des citoyens (protection des données personnelles et de la vie privée, surtout dans un monde de plus en plus numérisé (l'Internet des Objets et les mégadonnées («Big Data»); Sûreté de l'État (surveillance)

Règlement général sur la protection des données – entrera en vigueur en mai 2018, directive «Vie privée et communications électroniques», directive PNR et accords internationaux PNR; décisions en matière d'adéquation

Q4.1: Comment votre pays se prépare-t-il pour l'entrée en vigueur du règlement général sur la protection des données (RGPD) en mai 2018? Existe-t-il des propositions législatives spécifiques ou des mesures d'exécution en préparation?

Q4.2 : Comment les entreprises de votre pays s'adaptent-elles aux nouvelles exigences du RGPD telles que celles relatives au consentement, aux analyses d'impact, au respect de la vie privée dès la conception et par défaut?

Q4.3: Quelles sont les questions les plus controversées dans votre pays (d'un point de vue juridique) en ce qui concerne l'IdO (Internet des Objets) / les villes intelligentes / les données générées de machine à machine / voitures automatisées? (Des questions de propriété? Accès et utilisation ? Responsabilité en cas de préjudice ?) Existe-t-il des mesures législatives spécifiques ou des avis/décisions réglementaires dans ce domaine? Quel est l'état du débat politique?

Q4.4: Depuis l'arrêt controversé de la CJUE en mai 2014 dans l'affaire Google Espagne (ou Costeja), ce qu'on appelle le «droit à l'oubli» (ou à la radiation) a reçu beaucoup d'attention en Europe et au-delà. Quel est le statut légal dans votre pays? Des plaintes sont-elles portées devant l'autorité chargée de la protection des données et/ou les tribunaux? Y a-t-il eu une jurisprudence croissante à cet égard? Comment est atteint l'équilibre entre le droit de l'individu à la protection des données et les autres intérêts en jeu (en particulier la liberté commerciale du moteur de recherche, le droit du public à l'information et le droit de l'auteur à la libre expression)?

FRAGEBOGEN

Peggy Valcke*
Piedade Costa de Oliveira**

KAPITEL

1. Binnenmarkt und elektronischer Handel: Internet und E-Kommerz

E-Kommerz und Verbraucherschutz: Verantwortlichkeit der Vermittlungsdienstanbieter, Rechte der Verbraucher: Geoblocking; Internet-Kauf und Vertragsrecht; Verbraucherschutz und Streitbeilegung: "*Ökonomie des Teilens*".

Richtlinie über den elektronischen Geschäftsverkehr; Vorschläge zum digitalen Verbraucherschutz (bzgl. digitalem Inhalt und digitalen Verträgen für Waren).

2. Digitale media

Die Verteilung audiovisueller Inhalte über das Internet; Konvergenz mit den sozialen Media, (freie Meinungsäußerung, Hassreden); Geistiges Eigentum (eventuell beschränkt auf die Urheberrechte) im digitalen Bin nenmarkt; „AVMD" Richtlinie (wird überarbeitet); Urheberrechtsrahmen (wird überarbeitet)

3. Digitale Infrastrukturen

High speed networks, spectrum managment, Neutralität im Internet, Bürger und das Internet: Vernetzung für Alle, Zugang zum Web.

* Genereller Berichterstatter.
** Institutioneller Berichterstatter.

Rahmenregelungen für elektronische Kommunikation (wird überarbeitet), Richtlinie über den Zugang zum Web.

4. Daten in der digitalen Wirtschaft

„Daten als ein Gewinn": der freie Datenfluss und das Problem der Lokalisierung von Daten. Neu auftauchende Probleme (vor Allem im Kontext der digitalisierten Industrie und der Automatisierung): offene Daten, Daten, die von Maschine zu Maschine verarbeitet werden (z.B. Roboter, automatische Autos): Eigentum, Zugang und Gebrauch; Verantwortlichkeit im Schadensfall.

Die fundamentalen Rechte der Bürger (Schutz der persönlichen Daten und der Privatsphäre, besonders in einer mehr und mehr digitalisierten Welt (Internet „*Of Things and Big Data*"; Staatssicherheit Überwachung).

Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten – tritt Mai 2018 in Kraft; Richtlinie über die EPrivatsphäre, PNR Richtlinie und PNR internationale Übereinkünfte; Entscheidungen über die Angemessenheit.

THEMA 1: BINNENMARKT UND DIGITALE WIRTSCHAFT

Es ist allgemein bekannt, dass einer der wichtigsten Pfeiler der EU, der Binnenmarkt, auf tiefgreifende Weise von den aufgrund der technologischen Entwicklung hervorgerufenen Veränderungen betroffen ist.

Auf EU-Ebene wurden in verschiedenen Gebieten bereits existierende Gesetze vor Kurzem überarbeitet und neue wurden (oder werden es in naher Zukunft) hinzugefügt. Sie alle sind darauf ausgerichtet, den neuen, aus der schnellen technologischen Entwicklung und der Globalisierung stammenden Herausforderungen eine Antwort bieten zu können.

Die Kommission nahm im Mai 2015 die „*Strategie für einen digitalen Binnenmarkt für Europa*" an, die eine Aufstellung der größten Herausforderungen und wichtigsten Maßnahmen enthält.

Ein Teil dieser Maßnahmen wurde in sukzessiven „Paketen" ab Dezember 2015 angekündigt und können gemäß der in der „*Strategie für einen digitalen Binnenmarkt*" identifizierten Pfeiler in drei Gruppen unterteilt werden:

1) *Besserer Online-Zugang für Verbraucher und Unternehmen zu Waren und Dienstleistungen in ganz Europa – Hierzu müssen rasch die größten Unterschiede zwischen Online- und Offline – Umgebung beseitigt werden, damit grenzüberschreitende OnlineAktivitäten nicht länger behindert werden.*
2) *Schaffung der richtigen Bedingungen für florierende digitale Netze und Dienste – Dies erfordert hochleistungsfähige, sichere, vertrauenswürdige Infrastrukturen*

sowie Inhaltsdienste, die durch geeignete ordnungspolitische Rahmenbedingungen für Innovationen, Investitionen, fairen Wettbewerb und Chancengleichheit gestützt werden.

3) *Bestmögliche Ausschöpfung des Wachstumspotentials unserer europäischen digitalen Wirtschaft – Hierzu sind Investitionen in die IKT-Infrastruktur und in Technologien wie Cloud-Computing und Big Data sowie in Forschung und Innovation nötig, um die Wettbewerbsfähigkeit der Wirtschaft zu stärken, aber auch um die öffentlichen Dienste, Inklusion und Kompetenzen zu verbessern.*

Die Wahl der Unterpunkte des Thema 1 gründet sich nicht nur auf der Tatsache, dass die Gerichte sich heutzutage mehr und mehr mit diesen Themen beschäftigen müssen, sondern vor Allem darauf, dass diese Gebiete das Bedürfnis nach einer Neuformulierung der juristischen Konzepte und der Anpassung der gesetzlichen Rahmenregelungen an neue Realitäten und Herausforderungen aufzeigen.

FRAGEBOGEN

Binnenmarkt und digitale Wirtschaft

Dieser Fragebogen soll den Rahmen für nationale und institutionelle Berichte bzgl. der unten aufgeführten Unterpunkte bieten.

1. Binnenmarkt und elektronischer Kommerz: Internet und E-Kommerz

E-Kommerz und Verbraucherschutz: Verantwortlichkeit der Vermittlungsdienstanbieter, Rechte der Verbraucher: Geoblocking; Internet-Kauf und Vertragsrecht; Verbraucherschutz und Streitbeilegung; *„Ökonomie des Teilens"*.

Richtlinie über den elektronischen

Geschäftsverkehr 2003/31 EC; Vorschläge zum digitalen Verbraucherschutz (bzgl. digitalem Inhalt und digitalen Verträgen für Waren).

1.1. E-Kommerz und Verantwortlichkeit der Vermittlungsdienstanbieter

Kurze Einleitung: Die Richtlinie über den elektronischen Geschäftsverkehr hat Ausnahmen hinsichtlich der Verantwortlichkeit für diejenigen Anbieter festgelegt, deren Dienste auf den rein technischen Vorgang beschränkt sind, eine „reine Durchleitung", ein „Caching" darstellen; allerdings gilt hier die „notice-and-take-down" Regelung, die Mittler müssen unverzüglich nach Kenntnisnahme wirksame Maßnahmen zur Entfernung rechtsverletzender Inhalte ergreifen. Diese Regelungen sind nicht nur auf das geistige Eigentum beschränkt,

sondern beziehen sich auf alle Arten von Verantwortlichkeiten, das Strafrecht eingeschlossen. Verantwortlichkeitsprobleme und Gerichtsanordnungen haben zu einer Reihe von Entscheidungen des EUGH geführt[1]. Daher könnte der erste Unterpunkt die Frage nach der systematischen Relevanz des in der Richtlinie über den elektronischen Geschäftsverkehr enthaltenen Konzepts des Vermittlungsdienstanbieters und der Freistellung von der Verantwortlichkeit aufwerfen.)

F1.1.1: Mit welchen Schwierigkeiten (z.B. Definition, Abgrenzung) waren/sind Mitgliedstaaten und nationale Gerichte konfrontiert, wenn sie Gesetze verabschieden oder mit Fällen konfrontiert waren/werden, in denen das Konzept des Vermittlungsdienstanbieters in Frage steht?

F1.1.2: Hat der EUGH Ihrer Meinung nach im Fall L'Oréal gegen eBay, C-324/09, eine gute Untersuchung des Problems der Verantwortlichkeit vorgelegt?

F1.1.3: Ist das System von „notice-and-take-down" angebracht in allen Arten von Situationen (z.B. in Fällen von Verletzung der Rechte Dritter, wie z.B. Urheberrechte, durch ISS-Nutzer; Hassreden)?

Wenn nicht, wie könnten adäquate Lösungen aussehen?

F1.1.4: Mit welchen Schwierigkeiten waren/sind Mitgliedstaaten und nationale Gerichte konfrontiert, wenn sie bzgl. eventueller Anordnungen entscheiden müssen?

(Scarlet gegen SABAM C-70/10 und SABAM gegen Netlog NV C-360/10: Eine gerichtliche Anordnung bzgl. Filtersysteme im Gebiet der Urheberrechte würde mit anderen RechtsPrinzipien in Konflikt geraten können. Der EUGH hat jedoch eine Check-Liste für Anträge auf spezifische Sperrungen aufgestellt.)

[1] C-360/10 SABAM gegen Natlog NV, C-70/10 Scarlet Extended gegen SABAM, C-324/09 L'Oréal u.a. gegen eBay International A.G. u.a., C-236/08, C-237/08 und C-238/08 Google France und Google.Mc Fadden, C-484/14, 15.9.2016.
C-160/15, Schlussantrag des Generalanwalts, Paragraph 86: *Zwar bezweckt nämlich Art.14 der Richtlinie 2000/31 die Beschränkung oder die Befreiung der Fälle, in denen die Haftung von Vermittlungsdienstanbietern für Dienstleistungen der Informationsgesellschaft nach nationalem Recht ausgelöst werden kann, doch unterliegen die betroffenen Befreiungen strengen Beschränkungen. In diesem Zusammenhang hat der Gerichtshof in Rn.119 des Urteils L'Oréal u.a. (C-364/09 EU: C: 2011: 474) festgestellt, dass ein Anbieter von Hostingsdiensten (55) in einem Fall, in dem er sich auf rein technische und automatische Verarbeitung der Daten beschränkt hat, nach Art. 14 Abs.1 der Richtlinie 2000/31 von jeder Verantwortlichkeit für die von ihm gespeicherten rechtswidrigen Daten „nur dann freigestellt werden kann, wenn er keine tatsächliche Kenntnis von der rechtswidrigen Tätigkeit oder Information hatte und, in Bezug auf Schadensersatzansprüche, sich auch keiner Tatsache oder Umstände bewusst war, aus denen die rechtswidrige Tätigkeit oder Information offensichtlich wurde, oder wenn er, nachdem er diese Kenntnis oder dieses Bewusstsein erlangt hatte, unverzüglich tätig wurde, um die fraglichen Daten zu löschen oder den Zugang zu ihnen zu sperren".*

1.2. Verbraucherschutz in Bezug auf das Internet und den E-Kommerz, Internet-Käufe und Vertragsrecht; Verbraucherschutz und Streitbeilegung[2]

F1.2.1: Mit welchen Schwierigkeiten war/wird Ihr Mitgliedstaat konfrontiert, wenn Lösungen gemäß der Richtlinie zu bestimmten Aspekten des Verbrauchsgüterkaufs und der Garantien für Gebrauchsgüter gesucht werden?

F1.2.2: Bietet die vorgeschlagene Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte (COM (2015) 634) angemessene und ausreichende Regelungen zur Erreichung eines echten digitalen Binnenmarktes?

F1.2.3: Bietet die vorgeschlagene Richtlinie über bestimmte vertragsrechtliche Aspekte des Online-Warenhandels und anderer Formen des Fernabsatzes von Waren (COM(2015)635) und die vorgesehene vollständige Harmonisierung der vertraglichen Schlüsselrechte angemessene und ausreichende Regelungen zur Erreichung eines echten digitalen Binnenmarktes?

F1.2.4: Wie schätzen Sie die Auswirkungen der harmonisierten Regelungen bzgl. der Anwendung der oben genannten europäischen Verbraucherschutz-Regelungen ein?[3]

[2] Auszug aus SWD (2016) 163 Leitlinie zu UCPD
Die UGP kann nur in B2C Situationen angewandt werden. Der erste Schritt zur Prüfung der Anwendbarkeit dieser Richtlinie auf jedwelche Online-Plattformanbieter muss also die Frage sein, ob er ein „Gewerbebetreiber" i.S. von Artikel 2, Buchstabe b) UGP ist. Gemäß einer von Fall zu Fall Prüfung kann ein Plattformanbieter aus mit seinen Geschäftsangelegenheiten in Zusammenhang stehenden Gründen handeln, etwa wenn er eine Provision für den Geschäftsvorgang zwischen dem Anbieter und dem Benutzer verlangt oder zusätzliche, zu vergütende Dienste anbietet oder Einkommen aus gezielter Werbung erzielt.
Darüber hinaus darf kein Plattformanbieter, der „Gewerbebetreiber" i.S. von der UGP ist, gemäß Artikel 5 Absatz 2 UGP in seinen Geschäftspraktiken mit dem Verbraucher gegen die „berufliche Sorgfalt" verstoßen. Gemäß Artikel 2, Buchstabe h) UGP ist unter „berufliche Sorgfalt" der Standard an Fachkenntnissen und Sorgfalt zu verstehen, bei denen billigerweise davon ausgegangen werden kann, dass der Gewerbebetreiber sie gegenüber dem Verbraucher gemäß den anständigen Marktgepflogenheiten und/oder dem allgemeinen Grundsatz von Treu und Glauben in seinem Tätigkeitsbereich anwendet.
Die in UGP niedergelegte „berufliche Sorgfalt" dieser Gewerbebetreiber den Verbrauchern gegenüber ist, wenn auch komplementär, so doch zu unterscheiden von der Regelung der Freistellung von der Verantwortlichkeit gemäß Artikel 14 der Richtlinie über den elektronischen Geschäftsverkehr im Falle rechtswidriger Informationen, die auf Auftrag eines Dritten von einem Dienstanbieter gespeichert werden. Besonders Artikel 14 Absatz 1 wird häufig von Dienstanbietern eingewandt mit dem Argument, sie hätten lediglich als Anbieter von Informationsdiensten i.S. von Artikel 14 der Richtlinie über elektronischen Geschäftsverkehrs gehandelt und seien aus diesem Grund nicht für die von ihnen gespeicherten Informationen verantwortlich.
Darüber hinaus wird den Mitgliedstaaten gemäß Artikel 15 Absatz 1 keine allgemeine Verpflichtung dazu auferlegt, die von Anbietern von Diensten im Sinne von Artikel 12, 13 und 14 der gleichen Richtlinie übermittelten oder gespeicherten Informationen zu überwachen oder aktive Recherchen diesbezüglich zu führen.
[3] COM (2015) 635, p.7: Das Konzept der vollständigen Harmonisierung hat sich bereits im Bereich der EU-Verbraucherschutzvorschriften bewährt, zum Beispiel durch die in Richtlinie 2011/83/EU vorgese-

F1.2.5: Sind Sie der Meinung, dass das zur Zeit bestehende EU- Verbraucherschutzrecht (Richtlinie über unlautere Geschäftspraktiken 2005/29/EG; Richtlinie über missbräuchliche Klauseln in Verbraucherverträgen 1993/13/EG und die Richtlinie über die Rechte der Verbraucher 2011/83/EG) ausreichend und angebracht für den Schutz der Verbraucher im Bereich ihrer Tätigkeiten mit Online-Plattformen ist?

F1.2.6: Gab es vor Ihren nationalen Gerichten eingereichte Klagen, die sich, gestützt auf das Verbraucherrecht, gegen von Online-Dienstanbietern angewandte Klauseln und Bedingungen richteten?

F1.2.7: Glauben Sie, dass es sinnvoll/nötig ist, die Reichweite der Regelungen in Bezug auf den Handel mit Verbrauchern (B2C) auf den Handel mit Unternehmen (B2B) auszuweiten?

1.3. Geoblocking

Die Kommission hat einen Vorschlag über die Verhinderung von ungerechtfertigtem Geoblocking vorgelegt (COM(2016)289). Der Vorschlag definiert spezifische, nicht zu rechtfertigende Situationen von Geoblocking oder anderer, auf der Staatsangehörigkeit, dem Wohnsitz oder dem Ort der Niederlassung basierenden Diskriminierungen:

- Wenn ein Verbraucher Güter, wie z.B. elektronische Waren, Kleidung, Sportkleidung oder Bücher kauft, die der Anbieter nicht grenzüberschreitend zustellt;
- Wenn ein Verbraucher eine elektronische Dienstleistung erwirbt, wie z.B. CloudDienste, eine Data-Warehousing oder Webhosting;
- Wenn ein Anbieter Dienste bereitstellt und diese Dienste vom Kunden in den Räumlichkeiten des Anbieters oder in einem vom Anbieter gewähl-

henen Bestimmungen, die eine Reihe einheitlicher Verbraucherrechte für alle Verbraucher innerhalb der EU gewährleisten, welche in allen Mitgliedstaaten einheitlich ausgelegt und durchgesetzt werden. Eine Initiative auf EU-Ebene gewährleistet eine kohärente Entwicklung der Verbraucherrechte und stellt gleichzeitig sicher, dass alle Verbraucher in der EU das gleich hohe Verbraucherschutzniveau genießen. Sie schafft Rechtssicherheit für Unternehmen, die ihre Waren in anderen Mitgliedstaaten verkaufen möchten. Ein solches Ergebnis kann nur durch ein Vorgehen auf Ebene der EU erreicht werden.
Zudem gewährleistet eine Initiative auf EU-Ebene, dass die Verbraucherrechte kohärent angewandt werden und dass gleichzeitig alle Verbraucher in der EU das gleich hohe Verbraucherschutzniveau genießen. Sie schafft Rechtssicherheit für Unternehmen, die ihre Waren in anderen Mitgliedstaaten verkaufen möchten. Eine solche Initiative bildet eine schlüssige Rechtsgrundlage für koordinierte Durchsetzungsmassnahmen, da die vorgeschlagene Richtlinie in den Anhang der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden aufgenommen wird. Zudem würden die vorgeschlagenen, vollständig harmonisierten Vorschriften die Rechtsdurchsetzung erheblich erleichtern und den Verbraucherschutz in der EU stärken. Ein solches Ergebnis kann nur durch ein Vorgehen auf Ebene der EU erreicht werden.

ten Standort entgegengenommen werden, wie z.B. im Falle von Hotelunterbringung oder der Autovermietung.

Darüber hinaus untersagt der Vorschlag die Sperrung des Zugangs zu Websites und die automatische Weiterleitung von Kunden ohne deren ausdrücklicher Zustimmung.

Der Vorschlag sieht gleichfalls eine Regelung für den Bereich der Zahlungen vor. Auch wenn der Anbieter in seiner Wahl des Zahlungsmittels weiterhin frei ist, enthält der Vorschlag eine spezifische Regelung der Nicht-Diskriminierung innerhalb dieses gewählten Zahlungsmittels.

Mehr Informationen diesbezüglich: https://ec.europa.eu/digital-single-market/en/geoblocking-digital-single-market

Frage 1.3.1: Der Vorschlag (COM (2016) 289) hat die Verhinderung ungerechtfertigter, auf der Staatsangehörigkeit, dem Wohnsitz oder des Ortes der Niederlassung basierender Diskriminierung in grenzüberschreitenden Situationen zum Ziel. Wie verstehen Sie die Verknüpfung zwischen der oben genannten Verordnung und der Verordnung 1215/2015 bzgl. des Falles eines Anbieters, der seine Aktivitäten in einem anderen Mitgliedstaat ausübt, in welchem der Verbraucher seinen Wohnsitz hat?

1.4. Fragen in Bezug auf die kollaborative Wirtschaft (COM(2016)356

F1.4.1: Was sind die umstrittensten Gerichtsstreitigkeiten in ihrem Land, die von der kollaborativen Wirtschaft ausgelöst wurden?

F1.4.2: Wettbewersbsprobleme: Führt die Tatsache, dass solche Geschäftstätigkeiten in Märkte vordringen, die bis dato von traditionellen Dienstanbietern bedient wurden, zu Wettbewerbsproblemen?

F1.4.3: Marktzugangsanforderungen: Welche Art von Dienstanbieter, die in der kollaborativen Wirtschaft tätig sind, müssen gemäß der in Ihrem Staat herrschenden Regelungen eine Genehmigung hierzu haben? Was sind die Bedingungen zum Erhalt einer solchen Genehmigung? Sind die hierzu erforderlichen behördlichen Verfahrensweisen und Formalitäten klar und transparent?

F1.4.4: Verbraucherschutz[4]: Gibt es Probleme auf dem Gebiet des Verbraucherschutzes, die Gegenstand von Rechtsbehelfen in Ihrem Staat sind?

F1.4.5: Unter welchen Umständen gilt ein Anbieter in einer „Peer-to-Peer"-Dienstleistung gemäß Ihrem nationalen Recht als ein gewerblicher Dienstanbieter?

[4] EU Verbraucherrecht ist auf jedwelche kollaborative Plattform anwendbar, die als „Dienstanbieter" Geschäftstätigkeiten mit seinen Verbrauchern ausübt. Demgegenüber ist EU Verbraucherrecht und Marketing-Gesetzgebung nicht auf „Peer-to-Peer"-Dienste anwendbar

F1.4.6: Wie können gesetzliche Regelungen dazu beitragen, dass das Vertrauen der Verbraucher in „Peer-to-Peer"-Dienste gestärkt wird? Glauben Sie dass vertrauensstärkende Mechanismen wie das „online-rating" und andere Begutachtungssysteme und Gütezeichen die angebrachten Instrumente zum Überwinden des Informationsmangels im Bereich der individuellen Dienstanbieter sind? Welche anderen Instrumente würden Sie für angebracht erachten?

2. Digitale Media

Die Verteilung audiovisuellen Inhalts über das Internet; Konvergenz mit den sozialen Media (freie Meinungsäußerung, Hassreden); Geistiges Eigentum (evtl. beschränkt auf die Urheberrechte) im digitalen Binnenmarkt; „AVMD" Richtlinie (wird überarbeitet); Urheberrechtsrahmen (wird überarbeitet); Portabilität von Online-Inhalten

Der Mediensektor ist zur Zeit einer wesentlichen Veränderung unterworfen. Dies ist auf die Digitalisierung, rasante Entwicklung des Internet, Konvergenz sowohl zwischen gedruckter und audiovisueller Medien[5], als auch zwischen traditioneller und sozialer Medien, zurückzuführen.

Heutzutage können wir unsere beliebtesten Fernsehprogramme aus ganz Europa nicht nur im Fernsehen sondern auch auf unseren mobilen Geräten sehen. So wie andere Waren und Dienste auch, sind die audiovisuellen Medien den Regelungen des europäischen Binnenmarktes unterworfen. Die EU „Richtlinie über audiovisuelle Mediendienste" regelt die europaweite Koordination der nationalen Rechtsordnungen bzgl. aller audiovisueller Mediendienste, sowohl die der traditionellen Fernsehsendungen als auch die der auf individuelle Nachfrage erbrachten audiovisuellen Dienstleistungen. Zur Zeit wird die Richtlinie AVMD überarbeitet. Ein neuer Gesetzesvorschlag zur Änderung der AVMD Richtlinie wurde von der Europäischen Kommission am 25 Mai 2016 angenommen.

[5] *Verleger von Online-Zeitungen und Online-Zeitschriften sind mehr und mehr dazu übergegangen, Spots u.Ä. als ein Art von Zusatz zu den journalistischen Artikeln auf ihrer Website anzubieten. Häufig sind diese Spots in verschiedenen Orten der Website aufbewahrt und besitzen Navigationshilfen für den Gebraucher (wie z.B. die jüngsten Videos, die am meisten gesehenen Videos); sie können die gesamte Bandbreite der Reportagen umfassen. Die Unterscheidung zwischen Presseprodukten und den audiovisuellen Mediendiensten ist äußerst wichtig, da unterschiedliche gesetzliche Anforderungen und Regulierungssysteme zur Anwendung kommen. Herausgeber von Zeitungen, sei es in gedruckter Form oder Online, sind weniger strengen Regelungen unterworfen als die audiovisuellen Mediendienste, die ihrerseits den Regelungen der EU Richtlinie über audiovisuelle Mediendienste (AVMD) unterworfen sind. Aufgrund der Konvergenz der Medien sind die früher klaren Grenzen zwischen diesen beiden Bereichen allerdings verwischt worden. Der EUGH musste vor kurzem klarstellen, wie die Klassifizierung von Diensten durchzuführen sein könnte (New Media Online GmbH gegen Bundeskommunikationssenat; C-347/14).*

Gleichzeitig und ebenfalls im Kontext der Strategie für einen digitalen Binnenmarkt, arbeitet die Kommission an einer ehrgeizigen Modernisierung des EU Urheberrechtsrahmens. Ziel ist es, die EU-Regelungen bzgl. der Urheberschaft auf das digitale Zeitalter vorzubereiten. Die Kommission veröffentlichte am 9 Dezember 2015 eine Mitteilung über einen moderneren und gemeinschaftlicheren Urheberrechtsrahmen, zusammen mit einem Verordnungsentwurf zur Sicherstellung der grenzüberschreitenden Portabilität von Online-Inhaltsdiensten im Binnenmarkt. Ziel dieser gesetzgeberischen Initiative ist es sicherzustellen, dass Verbraucher, die Filme, Sportübertragungen, Musik, E-Bücher und Spiele kaufen oder abonnieren, auch dann Zugang zu diesen Produkten haben, wenn sie sich in anderen Mitgliedsstaaten aufhalten.

Eine zweite Reihe von gesetzgeberischen Vorschlägen, die im September 2016 angenommen wurde, zielt auf die Modernisierung des Urheberrechtsrahmens hin: der Hauptpunkt liegt auf einem weitreichenderen, verbesserten Zugang zu digitalen Inhalten in allen Mitgliedstaaten, auf der Annahme von Regelungen über Ausnahmen und Grenzen in der digitalen Welt und auf der Erreichung eines gut funktionierenden Urheberrechtsmarktes. Das Paket beinhaltet einen Verordnungsentwurf, der die Anwendung des Ursprungslandes der Sendung auf einige Online-Übertragungen und des Kabelverbreitungsrechts einführt (und so das spezifische Regime für Urheberlizenzen für Fernseh-und Radiosendungen über Satellit oder Kabel gemäß der Richtlinie 93/83/EEC ausweitet mit dem Ziel, den Zugang zu mehr Online-Fernseh-und Radioprogrammen von anderen Mitgliedstaaten zu erleichtern).

Mehr Informationen unter: https://ec.europa.eu/digital-single-market/en/copyright

F2.1: In seinem Urteil vom 21. Oktober 2015 im Fall *New Media Online GmbH gegen Bundeskommunikationssenat* (C-347/14) hat der EUGH festgestellt, dass der Begriff „Sendung" im Sinne von Artikel 1 Absatz 1, Buchstabe b) der Richtlinie über audiovisuelle Mediendienste dahin auszulegen ist, dass er die Bereitstellung kurzer Videos, die kurzen Sequenzen aus lokalen Nachrichten, Sport und Unterhaltung entsprechen, in einer Subdomain der Website einer Zeitung erfasst. Er hat gleichzeitig festgestellt, dass Online-Zeitungen nicht *per se* von dem Anwendungsbereich der AVMD ausgeschlossen sind. Wenn Betreiber audiovisuelle Inhalte zur Verfügung stellen, so können diese im Falle der Erfüllung der Testkriterien bzgl. der Hauptziele unter den Anwendungsbereich der Richtlinie fallen.

Handeln Ihre nationalen Behörden diesem Urteil gemäß? Wenn nicht: in welchen Bereichen weichen sie hiervon ab? Hat das Urteil des EUGH in Ihrem Land zu einer neuen Annäherung an das Problem geführt?

Link zum Urteil: http://curia.europa.eu/juris/liste.js?num=C-347/14 und zum

Pressebericht: http://curia.europa.eu/jcms/upload/docs/application/pdf/201510/cp150127en.pdf

Informativer Urteilskommentar von der Europäischen Rundfunkunion: https://www.ebu.ch/files/live/sites/ebu/files/News/2015/10/Case%20note%20New%20Media%Online.pdf

F2.2: Der Gesetzesvorschlag zur Änderung der AVMD Richtlinie bindet VideoPlattformen (wie z. B YouTube) in den Anwendungsbereich der AVMD-Regelungen ein. Sind Sie der Meinung, dass dies ein Schritt in die richtige Richtung ist? Wie weit sollte das Ausmaß der Einbeziehung solcher Plattformen gehen: nur insofern, als der Schutz Minderjähriger oder der Kampf gegen Hassreden in Frage stehen, oder auch, wenn es um die Regeln über die gewerbliche Kommunikation geht (wie Produktplazierung, Sponsoring, Werbung...)? Beinhaltet Ihre nationale Rechtsordnung bereits spezifische Regelungen in diesem Sektor bzgl. audiovisueller Plattformen?

F2.3: Eines der wichtigsten Streitgebiete in Bezug auf die Überarbeitung der AVMD Richtlinie bezieht sich auf das Prinzip des Ursprungslandes und das Kriterium der Gerichtsbarkeit. Gab es in Ihrem Land Streitigkeiten bzgl. der Anwendung des Prinzips des Ursprungslandes (in welchen die einschlägige Regulierungsbehörde versucht hat, audiovisuellen Dienstanbietern aus anderen Mitgliedstaaten gewisse Regelungen aufzuzwingen)? Gab es Probleme mit aus außerhalb der EU stammenden Anbietern, die Ihr nationales Publikum zur Zielgruppe hatten?

F2.4: In ihrer heutigen Form verlangt die AVMD keinerlei Unabhängigkeit und stellt auch keine andere Anforderungen an die Medien-Regulierungsbehorden – ganz im Gegensatz zum Telekommunikationssektor, dem Energiesektor oder im Falle der Datenschutzbehörden. Sind Sie der Meinung, dass die Einführung einer solchen Unabhängigkeitsanforderung für audiovisuelle Mediendienste auf EU-Ebene ein Schritt in die richtige Richtung wäre? Würde dies die Schaffung eines Binnenmarktes für audiovisuelle Mediendienste erleichtern? Existieren nationale, gesetzlich verankerte Hürden für derartige Anforderungen an MedienRegulierungsbehörden? Existieren Fälle von unlauterem politischen oder wirtschaftlichen Druck auf Medien-Regulierungsbehörden in Ihrem Land?

F2.5: Was waren die umstrittensten Fälle in Ihrem Land in Bezug auf die Anwendung von Sendungsrechten? (d.h.: Regelungen bzgl. gewerblicher Kommunikation wie z.B. Produktplazierung oder Sponsoring? Für Minderjährige ungeeignete Inhalte im Fernsehen? Verbreitung von Hassreden? Die Rolle des öffentlich-rechtlichen Fernsehens/Radios? Die wachsende Media-Konzentration?) Glauben Sie dass einige Gebiete mehr Harmonisierung durch die AVMD Richtlinie brauchen?

F2.6: Gab es in ihrem Land Initiativen, die auf das Angebot zielgerichteter (oder adressierbarer) Werbung im Fernsehen oder auf personalisierte Inhalte gerichtet war? Wenn ja, wie geschah das im Licht der Sendungs/Datenschutzrechtsnormen?

Gab es eine Art von Kooperation zwischen der Medien-Regulierungsbehörde und der Datenschutzbehörde? Glauben Sie, dass eine europaweit harmonisierte Annäherung hier angebracht wäre?

F2.7: Sind die spezifischen Regelungen für Urheberrechtslizenzen für Fernsehen und Radiosendungen durch Satellit und Kabel (gemäß der Richtlinie 93/83 EWG) nach wie vor in Ihrem Land gültig? Wurden ähnliche Regelungen auf die von Sendeunternehmen ausgestrahlte Online-Übertragungen angewandt?

F2.8: Was sind die hauptsächlichen Hürden in Ihrem Land bzgl. der grenzüberschreitenden Portabilität digitaler Inhalte? Sind Sie der Meinung, dass das Ursprungsland des Verbrauchers von dem Dienstanbieter regelmäßig überprüft werden sollte? Wenn ja, wie könnte eine solche Anforderung mit den Datenschutzgesetzen gemäß der DSGVO in Einklang gebracht werden?

3. Digitale Infrastrukturen

High speed networks, spectrum managment, Neutralität im Internet, Bürger und das Internet: Vernetzung für Alle, Zugang zum Web.

Rahmenregelungen für elektronische
Kommunikation (wird überarbeitet), Richtlinie für den Zugang zum Web.

Telekommunikationsnetze und Dienstleistungen bilden das Rückgrat unserer Informationsgesellschaft. In den letzten Jahrzehnten hat die EU einen harmonisierten Regelungsrahmen für elektronische Kommunikation adoptiert um so innerhalb des europäischen Binnenmarktes den Wettbewerb zu verbessern, Innovationen zu fördern und die Verbraucherrechte zu stärken. 2015 nahm sie Regelungen zur Neutralität im Internet (offenes Internet) an, die sie als eine „wesentliche Errungenschaft für den digitalen Binnenmarkt" bezeichnete. Die in der Verordnung EU 2015/2120 enthaltenen Regelungen bestimmen, dass im Prinzip jeder Verkehr gleichbehandelt werden muss und es jedem Bürger der EU möglich sein muss, Zugang zum offenen Internet zu haben und es den Zugangsanbieter ermöglicht werden muss, seine Dienstleistungen in einem hochwertigen, offenen Internet anzubieten. Gemäß dieser Regelungen ist das blockieren, unterdrücken und diskriminieren durch Internetzugangsanbieter in der EU verboten, mit drei Ausnahmen: zur Entsprechung von Gesetzgebungsakten der EU oder mit Unionsrecht in Einklang stehenden nationalen Rechtsvorschriften; zur Bewahrung der Integrität und Sicherheit des Netzes; zur Verhinderung einer drohenden Netzüberlastung. Außerdem sind die Nutzer frei, ihre bevorzugten

Apps und Dienste zu benutzen, unabhängig von der Wahl des Angebots, das sie abonniert haben.

Desgleichen hat die EU mehrere Initiativen ergriffen zur Förderung von Investitionen in die das *high speed* Internet unterstützende Breitbandnetzwerke. Im Rahmen der Strategie für einen digitalen Binnenmarkt nahm die Kommission im September 2016 eine Reihe von Maßnahmen (zusammen mit einem Vorschlag für einen neuen *European Electronic Communications Code*) an – das sogenannte „Vernetzungspaket (*connectivity package*)" – mit dem Ziel, die EU auf die vorderste Front der Internet Vernetzung zu befördern und eine europäische GigabitGesellschaft zu schaffen. Das Paket stimuliert zudem den Wettbewerb, stärkt den Binnenmarkt sowie die Verbraucherrechte und zielt auf vereinfachte, auf die Zukunft gerichtete Regelungen hin, die die Investitionsfreudigkeit von Unternehmen in neue hochwertige Infrastrukturen innerhalb der EU fördern.

F3.1: Gab es in Ihrem Land bereits Regelungen in Bezug auf die Neutralität im Internet vor der Annahme der Verordnung 2015/2120? Wenn ja, waren sie strenger oder weniger streng als die der Verordnung? Was ist die nationale Annäherung gegenüber Praktiken des Nullsatzes („*zero-rating*") (die nicht ausdrücklich von der Verordnung verboten werden)?

F3.2: Sollte die EU noch weiter gehen und einen Binnenmarkt für telekommunikative

Netzwerke oder Dienste schaffen (und z.B. ein europaweites Lizenzsystem einführen)? Haben Ihre nationalen Behörden spezielle Breitband-Regelungen angenommen? Wurden diese aufgrund einer EU-Intervention oder auf eigene Initiative hin eingeführt?

F3.3: Gibt es in Ihrem Land Rechtsprobleme bzgl. des *spectrum management*? Wenn ja, wie wurden sie beglichen?

F3.4: Wurden in Ihrem Land Fragen in Bezug auf die Unabhängigkeit der nationalen Regulierungsbehörden aufgeworfen? Wenn ja, führten sie zu Gerichtsstreitigkeiten? Wie wurden sie entschieden?

4. Daten in der digitalen Wirtschaft

„Daten als ein Gewinn": der freie Datenfluss und das Problem der Lokalisierung von Daten. Neu auftauchende Probleme (vor Allem im Kontext der digitalisierten Industrie und der Automatisierung): offene Daten, Daten, die von Maschine zu Maschine verarbeitet werden (z.B. Roboter, automatische Autos): Eigentum, Zugang und Gebrauch; Verantwortlichkeit im Schadensfall.

Die fundamentalen Rechte der Bürger (Schutz der persönlichen Daten und der Privatsphäre, besonders in einer mehr und mehr digitalisierten Welt (Internet „*Of Things and Big Data*"; Staatssicherheit (Überwachung).

Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten – tritt Mai 2018 in Kraft; Richtlinie über die EPrivatsphäre, PNR Richtlinie und PNR internationale Übereinkünfte; Entscheidungen über die Angemessenheit.

F4.1: Wie bereitet sich Ihr Land auf das Inkrafttreten der Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Mai 2018 vor? Werden bereits spezifische gesetzgeberische Vorschläge oder Exekutivmaßnahmen vorbereitet?

F4.2: Wie passen sich die Unternehmen in Ihrem Land an die neuen, von der Verordnung gestellten Anforderungen bzgl. der Zustimmung, Folgenabschätzung, eingebauter Datenschutz und Datenschutzfreundlichkeit an?

F4.3: Welches sind die umstrittensten Probleme in Ihrem Land (vom juristischen Standpunkt aus gesehen) in Bezug auf das IoT (Internet der Dinge/Allesnetz)/*smart cities*/Verarbeitung von Daten von Maschine zu Maschine/automatische Autos? (Eigentumsprobleme? Zugang und Gebrauch? Verantwortlichkeit im Schadensfall?) Existieren spezifische gesetzgeberische Maßnahmen oder regulatorische Ansichten/Entscheidungen auf diesem Gebiet? Was ist der Stand der politischen Debatte diesbezüglich in Ihrem Land?

F4.4: Seit dem umstrittenen Urteil des EUGH vom Mai 2014 im Fall Google Spanien (oder Costeja), erhielt das „Recht vergessen zu werden" (oder das Recht, von der Liste abgesetzt zu werden) viel Aufmerksamkeit, sowohl innerhalb der EU als auch weltweit. Was ist die Rechtslage diesbezüglich in Ihrem Land? Wurden Beschwerden oder Klagen vor Ihrer nationalen Datenschutzbehörde/nationalen Gerichten eingereicht? Gab es eine größere Anzahl von Klagen auf diesem Gebiet? Wie wird zwischen dem Recht des Einzelnen auf Datenschutz und den anderen Interessen, die in Frage stehen(insbesondere das der unternehmerischen Freiheit der Suchmaschine, das Recht der Allgemeinheit auf Information und das Recht des Autors auf freie Meinungsäußerung?) abgewogen?

GENERAL REPORT



GENERAL REPORT

Peggy Valcke*

Introduction

It is common ground that one of the most significant founding stones of the EU, namely the internal market, is heavily touched upon by the unprecedented changes brought by technological developments. At EU level, the European Commission adopted the Digital Single Market Strategy in May 2015, setting out the major challenges and key actions it considered would need to be addressed. Part of those actions were put forward in successive 'packages' from December 2015 onwards and may be grouped according to the three pillars identified in the Digital Single Market Strategy namely:

1) ***Better access for consumers and businesses to online goods and services across Europe*** *– this requires the rapid removal of key differences between the online and offline worlds to break down barriers to cross-border online activity.*
2) ***Creating the right conditions for digital networks and services to flourish*** *– this requires high-speed, secure and trustworthy infrastructures and content services, supported by the right regulatory conditions for innovation, investment, fair competition and a level playing field.*
3) ***Maximising the growth potential of European Digital Economy*** *– this requires investment in ICT infrastructures and technologies such as Cloud computing and Big Data, and research and innovation to boost industrial competiveness as well as better public services, inclusiveness and skills.*

* Professor of Law KU Leuven – CiTiP (Centre for IT & IP Law) – imec (BE), and visiting professor Tilburg University (NL) and Bocconi University Milan (IT).
The report was closed on 31 March 2018.

In several areas of law existing legal instruments have recently been reviewed and new ones have been (or will be) added. All of them are intended to address new challenges brought by rapid technological developments and globalisation. The Institutional Report discusses a selection of the different initiatives under each of the three pillars, together with the most recent developments of the legislative process, where applicable. It is striking that, in all three pillars, the EU legislator often resorts to the use of regulations as harmonising instrument, instead of directives, showing its aspiration to adopt uniform rules for the whole of the EU.

This report summarizes the responses received by the national rapporteurs in the period October 2017-January 2018 on the basis of a questionnaire prepared by the Institutional and General Rapporteurs.[1] The choice for the (sub) topics included in the questionnaire was guided not only by the fact that these are the ones on which courts are increasingly invited to decide on but also, and primarily, because those areas demonstrate the need to rethink legal concepts and to adapt the legal frameworks to new realities and challenges.

1. Internal Market and Electronic Commerce

This main part of this section covers topics in relation to (national transpositions of) the E-Commerce Directive,[2] focusing on liability of internet intermediaries. It also deals with consumer rights in the digital market which the EU legislator intends to reinforce through adopting rules on geo-blocking; internet purchase and contractual rights; consumer protection and dispute resolution.[3] Finally, it looks at national developments in relation to the sharing economy.

[1] Due to the special situation of Switzerland in relation to the EU, the Swiss report only covers subtopic 4 ('Data in the Digital Economy'). For the other subtopics, it refers to a number of documents, in particular the Interim analysis 'Switzerland and the digital single market of the EU' of 7.6.2017, prepared by the responsible departments within the framework of the implementation of the strategy 'Digital Switzerland', available from https://www.bakom.admin.ch/dam/bakom/de/dokumente/informationsgesellschaft/mise%20en%20oeuvre/DSM_EU-CH.pdf.download.pdf/DSM%20UE%20et%20cons%C3%A9quences%20pour%20la%20CH_DE.pdf.

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ* L 178 , 17 July 2000, p.1. Details about national implementations of the E-Commerce Directive can be found in: European Commission, Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), 2010, Contributions and Summary Report, available from http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm.

[3] See the Digital Consumer Rights proposals (on digital content and on digital contracts for goods) discussed in the Institutional Report.

1.1. E-Commerce and Intermediary Liability

The E-Commerce Directive has created a regime of liability exemptions ('safe harbours') for providers whose services qualify as 'mere conduit', 'caching' and 'hosting'. It provides the basis for a notice-and-takedown procedure for illegal or harmful content. This regime is not limited to intellectual property (like the DMCA in the United States), but extends to all kinds of responsibility issues, including criminal law. Liability issues and court injunctions have led to a series of decisions of the CJEU.[4]

Q1.1.1: Which difficulties (e.g. definition, delimitation) were/are your Member State and national courts confronted with when laying down rules or deciding cases where the concept of intermediary service providers is at stake?

In most countries, the provisions on intermediary liability in Directive 2000/31/EC have been transposed quite literally.[5] Some rapporteurs indicate that their national laws have adopted more detailed provisions regarding the obligations and safe harbours of internet intermediaries (e.g. specific rules on search engines, hyperlinking, blogs, social networks or – through a 2016 amendment of the German Telemediengesetz – WLAN operators). Although the Swedish E-Commerce Act of 2002 mirrors the liability exemptions in the E-Commerce Directive, it had already adopted in 1998 its Act on Responsibility for Electronic Bulletin Boards, which imposes an obligation on certain online intermediaries (i.e. those which provide or operate websites where users can post and read messages) to supervise their services and to remove messages with obviously unlawful content (such as incitement to racial hatred or child pornography).[6] Four rapporteurs highlight discrepancies between their national law and the Directive,

[4] See, in particular, CJEU, Joined Cases C-236/08, C-237/08 and C-238/08, *Google France and Google*, 23 March 2010, ECLI:EU:C:2010:159; Case C-324/09, *L'Oréal a.o. v. eBay International AG a.o.*, 12 July 2011, ECLI:EU:C:2011:474; Case C-70/10, *Scarlet Extended v. SABAM*, 24 November 2011, ECLI:EU:C:2011:771; Case C-360/10, *SABAM v. Netlog NV*, 16 February 2012, ECLI:EU:C:2012:85; Case C-291/13, *Papasavvas*, 11 September 2014, ECLI:EU:C:2014:2209; Case C-160/15, *GS Media v. Sanoma*, 8 September 2016, ECLI:EU:C:2016:644; Case C-484/14, *Mc Fadden v. Sony*, 15 September 2016, ECLI:EU:C:2016:689.

[5] The Polish law speaks of "service provided electronically" instead of "information society service", but, despite the semantic difference, it is widely accepted in the doctrine that the meaning of the two terms is synonymous.

[6] This provision is, however, not to be interpreted as imposing a general obligation to monitor or to actively investigate illegal activity (which is prohibited by Article 15 E-Commerce Directive). Instead, the 'supervisory' obligation may be fulfilled by setting up a simple complaints mechanism, according to the preparatory works of the BBS Act. The Swedish rapporteur notes that there is hardly any case law interpreting the BBS Act, making it hard to assess whether the Act has been effectively implemented or whether the concept of "Bulletin Board Systems", criticised in the doctrine for its lack of clarity, is too narrow or outdated. A recent Government-commissioned report of 2016 proposed to include also

e.g. CZ (hosting exception, but solved through a euro-conformal interpretation) and Croatia (unauthorised narrowing of liability exemption for hosting providers) and Poland (notion of service provider limited to persons acting at least incidentally in their professional activity and/or for profit, but solved through a teleological and pro-EU interpretation, and the hosting exemption which does not distinguish between the various legal bases of liability). Instead of limiting the prohibition of a general monitoring obligation to providers qualifying as 'mere conduit', 'caching' and 'hosting' providers, the Portuguese E-Commerce and Data Protection Act of 2004 applies this principle to all those who qualify as 'intermediary service providers'. Given the very broad legal definition of the latter notion, a disproportionately great number of actors (including also e-commerce hubs and social networks) are exempted from a monitoring duty, according to the Portuguese rapporteurs.

In the absence of a specific definition of 'intermediaries' in the E-Commerce Directive, however, national courts have struggled with defining the notion of intermediary service provider, and hence, with delimiting the material scope of application of the safe harbour provisions. The emergence of platforms taking up a more active role through linking, selection, prioritization, promotion or advertising – *i.e.* activities going beyond a "purely technical, automatic and passive nature" – gave rise to a *rich body of case law* in many countries.[7] It falls beyond the scope of this report to give an exhaustive overview of where national interpretations are coherent or divergent, but what transpires from the reports, is that national courts in general follow the guidance offered by the CJEU in cases like *Google France, L'Oreal v. eBay*, etc.

In considering the nature of the activities undertaken by ISPs, to establish whether they can benefit from the liability exemptions, national courts have introduced distinctions between *'active' and 'passive' hosting providers* (e.g. in Italy). They have applied stricter standards of liability when the functioning of digital platforms reveals a significant degree of interaction between the hosting provider and the activity or information stored on request of the recipient of the service (the Czech courts, e.g., have accepted liability of intermediaries/hosting providers for third party content posted on their platform, especially when the platform takes a rather active role, by encouraging and moderating discussions – referred to as 'active hosting'). The insertion of clauses within the terms and conditions of the service, or the organization and selection of the information provided by

unlawful threats and unlawful violations of privacy within the scope of the BBS Act, but not to defamation cases (see Swedish country report, under Q1.1.3).

[7] See, for instance, the overview of case law in relation to discussion fora, websites providing hyperlinks, online market places, and search engines in the Belgian country report. The German country report refers to "hundreds of court decisions".

customers, including by providing search tools enabling users to search for content by keyword or by indexing and selecting videos, have been considered as features indicating a larger degree of control over third parties' content and justifying an exclusion of the hosting provider from the liability exemption.

Video portals (such as YouTube or DailyMotion) have been the subject of court cases in France and Italy, resulting in diverging interpretations (even within the same country).[8]

National case law on internet intermediary liability often relates to *online news portals* and the question whether they should be held liable for third-party comments (from readers) in reaction to articles published by the portals (please note that the question whether the online news provider can invoke the liability exemptions for its own content has been answered in the negative by the CJEU in C-291/13, *Papasavvas*).[9] There seems to be consensus amongst national courts that such online news portals which provide content services and not passive intermediation service cannot be exempted *entirely* from liability for comments posted by their readers. Online portals providing online commentary possibilities are considered to be engaged in activities the nature of which is not merely technical, automatic, and passive, thus they cannot claim of having no knowledge or control over the information transmitted. While not being the author of the comments, the online news portal is nevertheless considered publisher of such comments given its financial interest in publishing the comments (as the revenue of sale of advertisement depends on the number of comments). It was the Estonian Supreme Court who set in 2009 a landmark precedent in this regard in the legal dispute involving the online news portal *Delfi*. It can be noted that the European Court of Human Rights (ECtHR) in 2015 – ruling in Grand Chamber – upheld the view that a large professionally managed Internet news portal run on a commercial basis can be held liable for not removing without delay after publication users' comments amounting to hate speech and speech inciting violence.[10] A combination of factors relating to the characteristics of the news por-

[8] Compare, for instance, the decision of the Court of Torino in relation to YouTube of April 7th, 2017 with the decision of the Court of Appeal of Rome a few weeks later (April 29th, 2017) involving a similar case against video-sharing platform Break Media, described in the Italian country report. See also: E. Apa, F. Frigerio and P. Cavallo, "Court of Appeal of Rome confirms that video-sharing platforms shall take down content even if the cease-and-desist letter does not include URLs", *IRIS* 2017-7:1/24; available from http://merlin.obs.coe.int/iris/2017/7/article24.en.html.

[9] CJEU, C-291/13, *Papasavvas*, 11 September 2014, ECLI:EU:C:2014:2209: *"The limitations of civil liability specified in Articles 12 to 14 of Directive 2000/31 do not apply to the case of a newspaper publishing company which operates a website on which the online version of a newspaper is posted, that company being, moreover, remunerated by income generated by commercial advertisements posted on that website, since it has knowledge of the information posted and exercises control over that information, whether or not access to that website is free of charge."*

[10] ECtHR, 16 June 2015, *Delfi v. Estonia*, http://hudoc.echr.coe.int/eng?i=001-155105.

tal (large, professional, commercial), of the comments concerned (clearly illegal, amounting to hate speech), of the commenter (who remained anonymous), of the sanction imposed by the national courts (moderate compensation) led the Court to the conclusion that there was *no* violation of Article 10 ECHR. Subsequent judgments confirm that the *Delfi* ruling should be interpreted narrowly, taking due account of the specific circumstances at hand. In *MTE and Index.hu* the ECtHR found that holding a self-regulatory body *(Magyar Tartalomszolgáltatók Egyesülete, MTE)* and an Internet news portal *(Index.hu Zrt)* liable for vulgar and offensive comments posted by their readers on their respective websites did amount to a violation of Article 10 ECHR. Although the comments were made anonymously (like in *Delfi*), the Court held that (contrary to what was the case in *Delfi*) they did not constitute hate speech but were related to a matter of public interest, using a style that was common in communication on many Internet portals, and only concerned the commercial reputational interests of a company (a real estate website).[11] Last year, in *Pihl v. Sweden,* the ECtHR further clarified the limited liability of operators of websites or online platforms containing defamatory user-generated content, by confirming that Article 8 ECHR does not require, at least not from small non-profit associations operating a website or online platform open for users' comments, the pre-monitoring of all content, nor to have an effective notice-and-take-down system installed.[12] The latter judgment may be relevant in a pending legal dispute in Estonia in relation to private blogs. The Estonian rapporteurs refer to a 2014 judgement by the Tallinn Circuit Court, obliging a blogger to remove statements that were considered false and to make a clear statement that his former claims were not correct. They note that, in this case, the Estonian Supreme Court asked a preliminary question related to the scope of liability of false information on the internet.[13]

Also the Austrian and Slovenian rapporteurs point to (potential) conflicts that may arise between safe harbour provisions (in e-commerce acts) and provisions imposing certain liability on online media (in media acts). Whereas the Slovenian courts have applied the liability exemptions regardless of whether the defendant was considered a media publisher or not, a recent amendment to the

[11] ECtHR, 2 February 2016, *MTE and Index.hu v. Hungary*, http://hudoc.echr.coe.int/eng?i=001-160314.
[12] ECtHR, 9 March 2017, *Pihl v. Sweden*, http://hudoc.echr.coe.int/eng?i=001-172145. For a critical commentary of the ECtHR's case law on intermediary liability, see: D. Voorhoof, "Pihl v. Sweden: non-profit blog operator is not liable for defamatory users' comments in case of prompt removal upon notice", *Strasbourg Observers*, 20 March 2017; https://strasbourgobservers.com, and the references included.
[13] Unfortunately, no reference was provided, and the General Rapporteur was not able to identify the relevant case on https://www.riigikohus.ee/et/eesti-kohtute-eelotsusetaotlused. On 17 October 2017, the CJEU delivered a preliminary ruling upon request from the Estonian Supreme Court in relation to jurisdiction in the case of internet publications (C-194/16), but it seems unlikely that this is the case referred to by the Estonian rapporteurs.

Media Act (adopted in March 2016) requires all media publishers who allow the public to post comments on their website to adopt commenting rules and to take down any comment that does not comply with these rules as soon as possible and no later than one working day after receiving a report of the inappropriate comment (leaving the definition of the content of those commenting rules, however, entirely to the media publisher's discretion). Since provisions of the Slovenian Media Act have to be applied in conjunction with the Electronic Commerce Market Act, it remains to be seen if and how these new rules affect the liability of online media for readers' comments.

Various rapporteurs (see e.g. the French and Spanish country reports) note that it is increasingly difficult to apply the principles in the E-Commerce Directive in a more and more sophisticated environment, in particular, when dealing with collaborative economy platforms and/or with online platforms that use complex *algorithms* to match supply and demand of services provided by third parties. A different degree of control is exercised by the platforms, that in some cases merely display potential service providers, in some cases filter them (by geographic area, price, etc.) without an active role in the review of the service provider, and in some cases take a more active role.

Legislators in France and Germany have reacted by adopting *new laws, clarifying the duties of online intermediaries.* The *French Digital Republic Act* (Law n° 2016-1321 of October 7, 2016)[14] introduces specific obligations for *online platform providers*, which are defined as businesses that offer to customers an online communication service to the public that 1) enables the ranking or referencing by means of a computer algorithm of content, goods or services that are offered or displayed online by third parties (e.g., search engines), or 2) allows parties to get in contact with one another in order to sell goods, offer a service, or exchange or share content, goods or services (e.g., online auction or shopping websites). The obligations imposed on these platforms mainly concern the provision to consumers of loyal, clear and transparent information (a.o. regarding general terms of use and the means used to rank, reference or de-reference content, goods or services available via the platform).[15]

Pursuant to the new *German Act to Improve Enforcement of the Law in Social Networks* ("NetzDG"),[16] specific forms of online intermediaries ("social networks",

[14] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique; available from: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746.

[15] In this context, it can also be noted that France has installed *administrative* procedures to request internet content and hosting providers to remove illegal content on, or block access to, sites containing child pornography and sites inciting or glorifying terrorism (see below, Q1.1.4).

[16] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG), 7 September 2017; available (including a non-official English translation) from: http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/NetzDG.html.

such as Facebook and Twitter) are under a duty to adopt particular complaints procedures regarding content that violates provisions of the German Criminal Code, to delete or block access to that content, and to report on their practices in this regard periodically to administrative authorities. Failure to abide by these conditions results in the imposition of severe administrative fines (up to €50m if they do not remove "obviously illegal" hate speech and other postings within 24 hours of receiving a notification, or (non-obvious) "illegal" content within seven days).

So there is a clear trend, both at Member State level and EU level (cf. institutional report), towards requiring internet intermediaries to exercise greater responsibility and due diligence in the way they manage their networks, platforms and systems, and towards a narrowing of their immunity for liability. Human rights organisations have expressed deep concerns that such legislative actions will severely undermine freedom of expression, and are setting dangerous precedents for other countries that more vigorously apply criminal provisions to quash dissent and criticism, including against journalists and human rights defenders.[17]

Q1.1.2: Do you think in L'Oréal v eBay, C-324/09, the CJEU has put forward a reasonable test for liability?[18]

Article 14 E-Commerce Directive seeks to restrict or exempt cases where intermediary information society service providers may be liable under national law. However, the exemptions in question are subject to strict conditions. In *Google France*, the CJEU made clear that, in order for an internet service provider to fall within the scope of the liability exemption in Article 14 E-Commerce Directive, it is essential that the role played by that service provider is *neutral*, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores. It added to this in *L'Oréal v. eBay* that, even in cases where the service provider has confined itself to a merely technical and automatic processing of data, it none the less cannot rely on the liability exemption if it was aware of facts or circumstances on the basis of which a *diligent economic operator* should have realised that the offers for

[17] See, for instance, Article 19, "Germany: Act to Improve Enforcement of the Law on Social Networks undermines free expression", 1 September 2017, https://www.article19.org/resources/germany-act-improve-enforcement-law-social-networks-undermines-free-expression/.

[18] As the Finnish rapporteurs rightly point out, the CJEU did not put forward a comprehensive test for liability, but a standard for *immunity from liability* (since the E-Commerce Directive does not harmonize the grounds of liability of ISPs, but merely the grounds for immunity from liability as defined in national law).

sale in question were unlawful and it failed to act expeditiously to remove, or disable access to, the information.

Although several rapporteurs consider the *diligent economic operator* standard as being appropriate (with some adding "at least when adopted"), criticism is voiced in a number of country reports, notably with regard to its *ambiguity* in relation to the degree of awareness that will render a service provider ineligible for immunity. The Irish report, for instance, notes that "*although this standard appears to be an intermediate one resting between actual and constructive knowledge, [bearing in mind that a standard of constructive knowledge may infringe Article 15 ECD] it has yet to be applied by Irish courts in the defamation context. The application of the "diligent economic operator" test therefore remains inherently uncertain under Irish law*".[19] In particular in a defamation context, the question of whether receipt of a complaint for hosting defamatory content fixes service providers with actual knowledge, or awareness, is particularly complex (since publication of a statement alleged to be defamatory is not *per se* unlawful if some recognised defence is available).

The Italian rapporteur even notes that the inherent ambiguity of the test resulted in parties relying on the judgment to argue in the opposite sense before national courts in the aftermath of *L'Oréal v. eBay*. The discretion that the CJEU left to national courts may result in inconsistent assessment of the intermediaries' activities and in national variations. The Finnish rapporteurs stress that this is likely to lead to unnecessary self-restraint on the part of ISPs and/or excessive claims on the part of intellectual property owners, and thus for example to potential chilling effects on freedom of expression. They call for a clearer definition of the parameters of liability / exemption from liability by the CJEU or in the applicable legislation. In the same vein, the Greek rapporteurs highlight the need for further clarification of the *diligent economic operator* test, which implies in their view a general monitoring obligation, in conflict with Article 15 of the E-Commerce Directive.

Equally, the Spanish rapporteurs consider that the time to review the test might be approaching, as the digital ecosystem is growing in complexity and online platforms are growing in sophistication, reach and market power. They put up a warning sign, though. Before increasing liability of intermediaries, it is necessary to have a good understanding of the services provided by the online platforms, the degree of control they have over the content/services they intermediate, and the technical capabilities they really have. *"As automatization plays a key role in the intermediation service (and the efficiencies are passed to final users),*

[19] Irish country report, p.3, with reference to: H. J. McCarthy. "Is The Writing on the Wall for Online Service Providers? Liability for Hosting Defamatory User-Generated Content Under European and Irish Law", *Hibernian Law Journal*, 2015, 14(1).

increasing liability might require a control that reduces efficiency in the operation of the platform or just proves to be technically impossible."[20]

The Finnish country report makes a plea for the CJEU and ECtHR to engage more intensely in developing the standards to assess the liability of hosting platforms.[21]

> *Q1.1.3: Is the regime of notice-and-takedown appropriate in all kinds of situations (e.g. in cases of infringement of others' rights, such as intellectual property rights, by costumers of ISSs; hate speech)? If not, what could be other appropriate solutions?*[22]

Article 14 E-Commerce Directive provides the basis for notice-and-takedown procedures, but does not further specify the conditions and procedures. Rather, the Directive suggests that voluntary agreements between trade bodies and consumer associations could specify notice and takedown processes, and that such initiatives should be encouraged by Member States. Most countries, however, have not adopted explicit rules regarding notice of infringement, take-down process or counter notice and put back. Such lack of explicit rules is prone to result in a *lack of clarity and legal certainty* (especially when compared to legal regimes with statutory rules, like in e.g. the United States). The vagueness surrounding notice-and-takedown procedures (what is 'actual knowledge', 'awareness', 'expeditious'...) is a recurrent theme in the country reports and is **criticised** by several rapporteurs. Unsurprisingly, the European Commission's 2010 consultation on the E-Commerce Directive demonstrated a strong demand to regulate notice-and-takedown procedures at EU level[23] (a view which is shared by several rapporteurs, see e.g. Malta). Despite confirmation of strong support for action at EU level during a 2012 public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries,[24] no concrete steps have been taken so far.[25]

[20] Spanish country report, p.2.

[21] As outlined under Q1.1.1, the ECtHR has indeed in previous years adopted a series of judgments which helped to define the scope of 'due diligence obligations' in relation to hosting content online.

[22] For a detailed discussion of existing notice-and-action mechanisms, see a.o.: C.J. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis, PhD thesis (promoter P.B. Hugenholtz), University of Amsterdam*, 2016, available from http://hdl.handle.net/11245/1.527223; A. Kuczerawy, *Private enforcement of public policy: freedom of expression in the era of online gatekeeping, PhD thesis (promoter P. Valcke), KU Leuven*, 2018 (forthcoming).

[23] European Commission, Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), Summary Report, available from http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm.

[24] http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet_en.htm

[25] See, e.g., A. Kuczerawy, "Intermediary Liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative", *Computer Law and Security Review*, 2015, Vol 31(1), 46-56.

As the Irish rapporteurs note, the idea of notice-and-takedown put forward by the E-Commerce Directive can be described as a compromise seeking to reconcile the effective protection of third parties' rights with the imposition of reasonable and proportionate obligations of intermediary service providers. At the same time, they note that the regime does raise difficult questions for ISPs and courts as regards the removal of infringing content, and in particular in the case of allegedly defamatory statements, in circumstances where the ISP may have no means of knowing whether those statements are in fact true. The Italian rapporteur underlines that claims to remove content that constitutes hate speech or defamation, except for manifestly illicit conducts, requires ISP to investigate the degree of permissible exercise of freedom of speech, that is subject to different standard of constitutional protection in the US and Europe. He continues that *"[t]his scenario may result in attributing to ISPs a quasi-constitutional role while handling complaints for the removal of content in the absence of a judgment of a court declaring the same to be illicit. This way, taking an extreme view, ISP would be required to exert a kind of collateral private censorship that, most likely, would support the existence of an editorial responsibility."* The Belgian rapporteurs highlight the *importance of adequate judiciary oversight* and suggest a progressive system in, in first instance, a quick and unilateral court procedure would be available to obtain a preliminary injunction to stop (at least temporarily) the distribution of the allegedly infringing content, followed by an adversarial procedure allowing the intermediary and, where relevant, the author of the content, to defend their rights and interests.

As the information society expands and new forms of online activities appear, a *more tailor-made approach* seems appropriate, whereby notice-and-takedown measures are more diversified in light of the (potential) harm and the type of remedy sought, and are complemented by actions against repeat infringements as well as preventive measures.

The Finnish and Croatian country reports discuss the idea suggested in the literature[26] to establish different types of notice-and-action procedures for different types of infringing content (e.g. an automatic notice-and-takedown procedure for manifest hate speech and child pornography[27], versus a notice-and-notice procedure for copyright infringements[28]). The Hungarian rapporteurs suggest

[26] E.g. C. Angelopoulos and S. Smet, "Notice-and-fair-balance: how to reach a compromise between fundamental rights in European intermediary liability", *Journal of Media Law*, 2016, Vol.8, No.2, (266-301) 292.

[27] Which is already the case in Finland (see the Finnish country report and Swiss Institute of Comparative Law, 'Blocking, Filtering and Take-Down of Illegal Internet Content', 2015).

[28] As implemented by Canada in their 2010 digital copyright reform (see the Finnish country report for more details).

the introduction of a graduated response system (in addition to other mechanisms that could complement the notice-and-takedown procedure).

Since one of the main problems with the current regime is the high likelihood that a notice will result in the removal of the reported content, even though the hosted content is perfectly legal,[29] the suggestion has been made in the literature (as noted in the Croatian report) that the party who submits unfounded copyright notices is to be held liable for the damages caused by wrongful removal of legal content, with a view of preventing abuses of the current notice-and-takedown system.[30]

In a number of countries, national legislators have adopted specific regimes in the area of *copyright* ('*graduated response*' or '*three-strike*' procedures), entailing the possibility for right holders and their representatives to submit notice-and-takedown orders before administrative bodies (HADOPI in France, AGCOM in Italy, the Intellectual Property Commission in Spain, the Committee for the notification of online copyright infringements in Greece). The Portuguese E-Commerce and Data Protection Act contains a basic provision on notice-and-takedown, but was never further implemented through secondary legislation (as foreseen by the Act). To fill the gap, a particularly interesting and, according to the rapporteur, unique self-regulation mechanism has been set up through the Memorandum of Understanding of 30 July 2015 signed by the General Inspectorate for Cultural Activities ('IGAC'), the Portuguese Association of Telecommunication Operators ('APRITEL'), the Civic Movement Against Online Piracy ('MAPINET' – a group representing several copyright holders in Portugal) and the DNS.PT Association (that is in charge of registrations in the .pt top-level domain, among others). It describes the conditions under which access to websites may be blocked in case of copyright breaches. The system, however, raises concerns over due process and legitimacy of blocking orders.

The Polish Ministry of Internal Affairs and Administration published in 2011 a draft bill which would introduce a dedicated notice-and-takedown mechanism in the Act of the Provision of Electronic Services, comparable to the one in the US Digital Millennium Copyright Act. According to the rapporteur, the proposed mechanism was however completely arbitrary and risked to be used as a powerful tool for censorship. It completely neglected any safeguards that the DMCA installs to prevent abuses (such as liability for false claims). The proposed bill was, however, never adopted.

[29] Commission Staff Working Document, Online services, including e-commerce, in the Single Market (COM(2011) 942 final, of 11.1.2012., p. 45.

[30] Patrick Leersen, The Limits of Limited Liability under Article 14 of the E-Commerce Directive – How 'Notice and Takedown' sidelines the use of copyright exemptions, Maastricht Student Law Review (2014)1, p. 13, http://www.mslawreview.eu/wp-content/uploads/2014/12/Leersen.pdf.

Extended withdrawal injunctions (the so-called '*notice and keep off*' or '*notice, take-down & stay-down*'), intended to prevent the recurrence of blocked or suppressed content, are controversial in some countries, even if the Court gave positive indications to that effect in *UPC Telekabel Wien* (see below). In the *Allostreaming* case, the Tribunal de Grande Instance of Paris ordered, for a period of twelve months, blocking measures, but did not grant the request of copyright holders to allow them to use a tool that they had conceived allowing the update of the injunctions of the court.[31] The French rapporteurs note that, similarly, in three judgments concerning Google, the Court of Cassation has censored an obligation to prevent reposting of the infringing content ('notice-and-staydown').

Italian courts have adopted several decisions requiring hosting providers to implement specific systems or software aimed at preventing users from uploading *ex novo* the same content previously subject to take down measures. Recently, on 8 May 2017, the Court of Milan specifically mentioned the CJEU's *Scarlet* case in order to justify the injunction against an online platform ordering it to take the necessary steps to avoid the repetition of the copyright infringements at hand. The Court of Turin, likewise, in its judgment of 7 April 2017, ruled that YouTube had to continue using the Content ID software. Apparently, the courts consider such requirement not contrary to the prohibition of general monitoring measures in Article 15 E-Commerce Directive. Where the CJEU in *Scarlet v. SABAM* and *SABAM v. Netlog NV* highlighted the need to strike a fair balance between copyright protection, on the one hand, and the protection of freedom of speech, personal data and freedom to conduct business, on the other one, Italian courts tend to refer to these criteria (among others, the Court of Rome in a judgment of 15 July 2016) to *support* the adoption of measures for copyright enforcement as a proportionate remedy, whose interference with the protection of other fundamental rights is not considered overbroad and excessive.

Finally, it is worth mentioning that also in the context of the protection of *personality rights* courts in Europe have ordered hosting providers and search engines to take measures in order to prevent the re-appearance of infringing content (such as filtering software, software for image recognition; erasure or blocking of content). The court cases against Google won by Max Mosley in France and Germany are landmark decisions in this regard and have received international attention.[32] The Greek country report refers to another decision

[31] The case has been commented extensively online, see e.g.: http://www.ipnews.be/france-analyse-de-la-decision-allostreaming/; https://www.legalis.net/actualite/les-fai-et-moteurs-de-recherche-sommes-de-bouter-hors-de-france-la-galaxie-allostreaming/.

[32] TGI Paris, 6 November 2013, RG 11/07970, Max Mosley v. Google Inc and Google France (available from http://droitdu.net/2013/11/tgi-paris-17e-ch-6-novembre-2013-rg-1107970-max-mosley-c-google-france-et-google-inc/); Landesgericht Hamburg, 24 January 2014, Az. 324 O 264/11 (available from

involving Google: in Case 457/2016 the Civil Court of Athens (First Instance) considered Google liable for offensive comments in blogs hosted through its services, although it had taken down the illegal content upon notice. However, it had not removed all files containing the infringing text. The Court imposed a notice-and-staydown measure, to prevent reposting of the offensive text. The Greek rapporteurs are critical of such measure, which in their view boils down to a general monitoring and filtering obligation, resulting in a disproportionate burden on intermediaries.

Q1.1.4: Which difficulties were/are your Member State and national courts confronted with when considering injunctions?

In several EU countries, most of the controversies and court cases have been about (preliminary) injunctions, notably the extent to which they can be invoked to remove infringing websites or block access to websites, and whether they can be used against intermediaries whose service is not infringing as such, but facilitates such infringement.[33] These aspects have hardly been harmonised at EU level – apart from the obligation for Member States to provide for injunctions against intermediaries in the case of intellectual property infringements (Articles 9(1)(a) and 11 Enforcement Directive 2004/48/EC, and Article 8(3) Infosoc-Directive 2001/29/EC) and the prohibition of a general monitoring obligation in Article 15 E-Commerce Directive. Disputes that arose between copyright holders and internet intermediaries in Belgium, respectively in Austria, have given the CJEU the opportunity to clarify certain aspects of those rules. In C-70/10, *Scarlet v. SABAM,* and C-360/10, *SABAM v. Netlog NV,* the CJEU ruled that the pronouncement of injunctions could not result in imposing on an internet service provider or a hosting service provider an obligation of permanent and generalized surveillance of information passed via its services, respectively hosted on its servers, which would disproportionately affect the freedom of enterprise of technical service providers and the freedom of communication.[34] In C-314/12, *UPC Telekabel Wien* the CJEU found that an internet service provider must be

https://openjur.de/u/674344.html). For more information, see e.g. https://globalfreedomofexpression.columbia.edu/cases/lg-hamburg-google-judgment/.

[33] For a detailed analysis of relevant national and EU case law in relation to the blocking of websites for copyright reasons, see: P. Savola, "Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers", *JIPITEC,* 2014, Vol.5, No. p.116-138.

[34] This reasoning has been followed by national courts. The French Court of Cassation, for instance, held in a judgment of 12 July 2012 that injunctions should be limited to measures preventing or stopping the damage related to the current content of the site in question, but excluded any measure of monitoring and filtering of illegal future content and any unlimited blocking device.

regarded as an intermediary within the meaning of Article 8(3) of Directive 2001/29/EC, against which an injunction can be issued.

The CJEU's rulings are generally followed by national courts. The French Court of Cassation, for instance, held in a judgment of 12 July 2012 that injunctions should be limited to measures preventing or stopping the damage related to the current content of the site in question, but excluded any measure of monitoring and filtering of illegal future content and any unlimited blocking device. The Swedish Patent and Market Court of Appeal found in its judgment of 13 February 2017 (*B2 Bredband* – also known as *Bredbandsbolaget*) that, despite the wording of "contribute" in Section 53b of the Copyright Act (to be understood in the criminal law sense according to the preparatory works), it was possible to issue an injunction against an intermediary whose services are used to commit a copyright infringement, even if the intermediary only provides internet access to its customers.[35] Referring to *UPC Telekabel Wien* the Swedish Court of Appeal rejected the view developed in the Act's preparatory works that some kind of special relationship had to be established between the intermediary and the third-party infringer.

Nevertheless, the EU legislative framework does not clarify the specific conditions under which injunctions must be issued, but *"only set[s] the outer boundaries within which injunctions may be issued",* as the Dutch rapporteurs eloquently phrase it. They note that their national legislation implementing these vague rules equally fails to add any additional conditions, procedures, limitations or safeguards that might allow for a more predictable balancing of the relevant competing fundamental rights (e.g. freedom of expression, privacy, intellectual property, freedom to conduct a business). The same observation is made by several other rapporteurs: injunctions are either based on general principles (general duty of care in tort law, or contributory liability in criminal law), or on provisions introduced in IP laws pursuant to Articles 9(1)(a) and 11 Enforcement Directive 2004/48/EC, and Article 8(3) Infosoc-Directive 2001/29/EC. According to its rapporteurs, Finland is one of the few countries which adopted detailed statutory rules concerning injunctions in its Copyright Act, when transposing Article 8(3) of Directive 2001/29/EC.[36]

Consequently, given the absence of detail in statutory law at both EU and national level, rules on what types of injunctive relief are available, in what kinds

[35] Swedish Patent and Market Court, 13 February 2017, Case PMT 11706-15, *Bredbandsbolaget*. See: https://www.worldipreview.com/contributed-article/blocking-copyright-infringement-online.

[36] According to Section 60 c of the Finnish Copyright act, the court may order the service provider acting as an intermediary to discontinue, on pain of fine, the making of the allegedly copyright-infringing material available to the public (injunction to discontinue). Finnish courts have issued injunctions based on this section on multiple occasions, such as in the case against *Elisa Corporation* (see footnote 33).

of cases and under what conditions, must necessarily be contested in individual court cases. This process of finding appropriate injunctions and their modalities is, however, a time-consuming process, as is illustrated by the (lengthy) legal proceedings in various countries with regard to the duty of access providers to block the controversial Swedish filesharing site '*The Pirate Bay*'.[37] In the Netherlands, the proceedings started in 2010 and, as of writing, have not yet come to a final conclusion after the CJEU's preliminary ruling in C-610/15, *Stichting Brein v. Ziggo and XS4ALL*.[38] In its judgment, the Court ruled that The Pirate Bay is a directly infringing website, which implies that under Article 8(3) of Directive 2001/29/EC and Article 11 of Directive 2004/48/EC, there is scope for obtaining an injunction against intermediaries, such as ISPs, which facilitate the infringing acts of third parties.

In Finland[39] and Belgium[40] injunctions issued against ISPs to block, by all technical means, all domain names leading to The Pirate Bay and to prevent access to the IP addresses used by The Pirate Bay, have been upheld by the highest courts.

By contrast, Norwegian and Swedish courts initially rejected blocking orders because the mere provision of internet access by the ISPs was not considered to

[37] The following paragraphs discuss the proceedings in Belgium, the Netherlands, Finland, Sweden and Norway on the basis of the information in the country reports. Please note that also in Denmark, Italy and the United Kingdom, courts have issued blocking orders in relation to The Pirate Bay; see B. Sookman, "Keeping The Pirate Bays at Bay: using blocking orders to curtail infringements", 22 February 2012, available from http://www.barrysookman.com/2012/02/22/keeping-the-pirate-bays-at-bay/.

[38] CJEU 14 June 2017, case C-610/15, *Stichting Brein v. Ziggo and XS4ALL*, ECLI:EU:C:2017:456. Awaiting the final decision by the Hoge Raad der Nederlanden, Stichting Brein obtained from the Court in The Hague a preliminary injunction ordering Ziggo and XS4ALL to block access to The Pirate Bay website(s); Rechtbank Den Haag, decision of 22 September 2017, ECLI:NL:RBDHA:2017:10789, available from https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2017:10789.

[39] Supreme Court of Finland, 29 October 2012, No 2187, *IFPI v. Elisa Corporation*. An interim injunction was found necessary by the Finnish courts in the view of the evidence on the effectiveness of legal measures and the accessibility of the alleged infringer. The Helsinki District Court also stated that the interim injunction may become long term if the defendants in the main issue cannot be summoned, but that this would not per se render the order unlimited in duration. See: http://merlin.obs.coe.int/iris/2013/1/article18.en.html.

[40] Court of Cassation, 22 October 2013, Case P.13.0550.N, *Telenet et al., Pas.*, 2013, p.2005. The Belgian Court of Cassation considered that such order did not constitute a general monitoring obligation in the sense of Article 15 E-Commerce Directive. Also the argument of the ISP, that Articles 35 to 39*bis* of the Code of Criminal Procedure only envisage fact-finding, but are not intended to prevent further perpetrations of such alleged infringements, was dismissed by the Court. The latter found that the Articles cited can be used not only for fact-finding, but also to stop certain acts which appear to constitute a criminal offence, or to protect civil interests. See: https://www.lexgo.be/nl/artikels/ip-it-telecom/informaticarecht/belgian-court-of-cassation-confirms-that-isps-can-be-requested-to-block-all-domain-names-leading-to-a-certain-website,83493.html.

qualify as the "contributory liability" required for preliminary injunctions.[41] In a landmark decision of November 2015, the District Court of Stockholm rejected an application by rightholders (including Universal Music, Sony Music Entertainment, Warner Music, Nordisk Film, and others) to issue an injunction against Swedish internet access provider *Bredbandsbolaget* (B2) to block access to torrent sites The Pirate Bay and Swefilmer.[42] The decision was, however, overruled by the Patent and Market Court of Appeal in 2017, which gave an EU conforming interpretation of the Swedish Copyright Act (see above).

The Norwegian courts only changed position after a legislative reform. Before, courts had found that the general rules on preliminary injunctions did not provide for a ground to compel Telenor to block access to The Pirate Bay's domain names (as Telenor could not be held liable for contributory infringement to the sharing of copyrighted material that was facilitated by The Pirate Bay). After the amendment of the Norwegian Copyright Act in 2013, the rightholders filed a new motion before the District Court of Oslo, this time with success. The Court ordered Telenor and other telecommunications providers to block *thepiratebay.se*, *piratebay.net*, *piratebay.org* and similar domain names and prevent them from being accessed by their customers. However, it rejected the rightholders' request to install a procedure to prevent 'domain name shuffle' (where a site changes its domain name to a new one once the old one is blocked), since the Copyright Act requires a new order for additional domains to be added to the list of blocked domains.[43]

Spanish Courts have also not hesitated to adopt interim measures asking telecommunications operators to block access to web pages and mobile apps in order to make third party rights effective *beyond intellectual propriety rights* (unfair competition, terrorism, child porn, etc.). Such requests have been made even in relation with content hosted in another Member State of the EU. A good example is the interim measure adopted *in audita parte* by Commercial Court no. 2 of Madrid against Uber on December 9, 2014.

In Portugal, a recent injunction was issued ordering Twitter to withdraw from its messaging service the unauthorised use of the claimant's logo.

[41] Also in Poland, an attempt to block a popular allegedly 'pirate' website was unsuccessful. The District Court in Warsaw claimed that the ISPs were not parties to the legal dispute (between rightholders and individuals who uploaded protected content on a 'pirate' website) and could therefore not be subject to a blocking order. The ruling raised questions about the compatibility of the Polish injunction system with EU law.

[42] District Court of Stockholm, 27 November 2015, Case T 15142-14, *Bredbandsbolaget*; available from http://www.stockholmstingsratt.se/Domstolar/stockholmstingsratt/Dokument/Stockholms%20TR%20T%2015142-14%20Dom%202015-11-27.pdf. See: http://ipkitten.blogspot.be/2016/03/stockholm-district-court-refuses-to.html .

[43] Order of Oslo District Court of 1.9.2015, TOSLO-2015-67093.

In 2014, France even installed an *administrative* procedure for blocking access to sites inciting or glorifying terrorism,[44] like it had done before in relation to child pornography sites. The Council of State confirmed the legality of the decrees taken in application of Article 12 of the Law of 13 November 2014: it does not follow from Article 10 ECHR that such measures may be ordered only by a judge; the mechanism pursues a legitimate aim; and appropriate safeguards are foreseen (including the transmission of the list of e-mail addresses to be blocked or dereferenced to a qualified person appointed by the CNIL and the obligation for the administrative authority to update quarterly the notified e-mail addresses).

It is worth noting that several country rapporteurs take a *critical* approach towards these developments (see also above, Q1.1.1). The Finnish rapporteurs, for instance, note that their courts have often neglected interests other than those of right owners in copyright blocking order cases, like the one described above in the case *IFPI v Elisa* (involving The Pirate Bay). Although such blocking orders are legally-technically speaking interim measures, their aim (and effect) has often been permanent blocking. Moreover, such measures could constitute *ex ante* restriction of freedom of expression (which is prohibited by section 12 of the Finnish constitution).[45]

In the same vein, the Spanish rapporteurs stress that web (or app) blocking should not be the response to potential infringements online. Notice-and-take-down and the suspension of the hosting service are more proportionate, particularly taking into account the risk of over-blocking (blocking access to legal content), the bypass to simple blocking measures (DNS filtering) and the high cost of more effective blocking measures. Only when notice-and take-down and suspension of hosting are not effective, blocking of websites should be considered. They continue that, in particular, interim measures ordering the blocking of webs and apps hosted in another Member State should be limited, as they seem contrary to the digital single market.

Also in Greece takedown requests have led to controversial decisions, but lately seem to be rejected more often.[46] The blocking of access to a specific website where also legal content may be available is considered not compatible with the principle of proportionality[47] and clashes with the freedom of information, the freedom to conduct a business and the right to participate in information society.

[44] Article 12 Loi nº 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, amending Article 7 Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (for an English translation, see: https://rm.coe.int/168045d73d).

[45] The rapporteurs indicate that the case law may change in the future due to recent legislative changes in the Finnish Copyright Act.

[46] Civil Court of Athens, First Instance, Cases No 13478/2014, 10452/2015.

[47] In Case No 13478/2014 the Civil Court of Athens (First Instance) following CJEU in case C-557/07 (LSG v. Tele2) points out that a consistent interpretation of relevant directives (2000/31, 2001/29,

Finally, some country reports discuss the question whether injunctions can be used in civil or criminal cases for the *disclosure of information about (the identity) of internet intermediaries' users.* The Belgian Court of Cassation opposed such a measure, at least in the context of civil proceedings, considering that the E-Commerce Act *"does not confer on a person who claims to be the victim of defamatory statements published on the site of a service provider the subjective right to obtain a court order obliging the service provider to provide him with all the information he has on the alleged perpetrators for the purposes of pursuing a civil action for damages".*

The Irish courts have considered the granting of such injunctions in the context of both copyright infringement and defamation cases. In doing so, they have upheld the use of Norwich Pharmacal orders[48] against Internet hosting services and Internet service providers to identify users which have allegedly engaged in wrongdoing and for "graduated response" notification systems (e.g. "three strike" scheme). In *Sony & Ors v UPC,* for instance, the Irish High Court granted an injunction requiring the defendant to operate a notification scheme (at its own expense) which would consist of the sending of "cease and desist" letters by the ISP to its customers following the notification by the plaintiff of a detected infringement. After a third notification by the plaintiff, the ISP would disclose the fact that two notifications had already received, so enabling the plaintiff to apply for a Norwich Pharmacal order for disclosure of the identity of the account holder.

The Dutch rapporteurs equally point out that the disclosure of information about an intermediary's customer who has allegedly used its services to disseminate unlawful content has regularly been sought through (preliminary) injunction orders. In a landmark decision from 2005, the Dutch Supreme Court held that a hosting provider could be ordered to disclose user data if it was: (a) sufficiently likely that the hosted information was unlawful and damaging to the claimant; (b) the claimant had a sufficiently clear interest in obtaining the user data; (c) no less invasive means to obtain the user data were available; and (d) the claimant's interests outweighed those of the provider and the user.[49] Although the Supreme Court explicitly limited this rule to the issue of obtaining name and address details from hosting providers, the same criteria have subsequently been used to order the provision of other kinds of information and from other kinds of intermediaries. The Dutch country report continues by pointing out a pressing

2002/58 and 2004/48) must not conflict with fundamental rights and general principles of Community Law, such as the principle of proportionality.

[48] A Norwich Pharmacal order is a court order whereby the defendant, albeit an innocent party, is ordered to disclose information because a civil wrong is being, or was being, perpetrated against the plaintiff and the defendant, though not a party to the wrong, can identify the tortfeasor.

[49] HR 25 November 2005, ECLI:NL:HR:2005:AU4019 (Lycos/Pessers).

issue that may arise when applying these criteria, also in light of the CJEU's ruling in *Bonnier Audio*,[50] notably the extent to which the claimant demanding identifying information must provide clear evidence that the user has indeed acted unlawfully (which is generally difficult for the intermediary to assess without involving the user in the proceedings, yet Dutch civil procedure does not provide for a procedure similar to US John Doe proceedings, in which an anonymous person can appear in proceedings to defend his right to maintain anonymity).[51]

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Q1.2.1: Which difficulties were/are your Member State and national courts confronted with when considering remedies under the Consumer Sales and Guarantees Directive? ("CSG Directive")

Although several rapporteurs list interpretation issues and describe extensive case law at national level, no major difficulties were encountered when considering remedies under the (national rules transposing the) CSG Directive. Contentious issues concerning remedies relate, for instance, to the extent a consumer can demand a replacement of a faulty good or has to settle for a repair (e.g. in Norway, Slovenia). In several countries, the legislator (e.g. the Netherlands) or the courts (e.g. Italy) have extended the time limits set by the CSG Directive in which remedies for non-conformity are available and/or in which a presumption of non-conformity applies to the benefit of the consumer. Also in Sweden a recent government-commissioned report found the period of six months in Article 5(3) CSG Directive (pursuant to which *"[u]nless proved otherwise, any lack of conformity which becomes apparent within six months of delivery of the goods shall be presumed to have existed at the time of delivery"*) too short and proposed an extension to two years. Legal conflicts have also arisen in relation to questions on determining conformity of goods sold (e.g. in Portugal).

[50] CJEU 19 April 2012, case C-461/10, par. 56-60.

[51] The Dutch country report describes how the District Court of The Hague provided an innovative approach by awarding an order to disclose user data that was suspended for two weeks to enable the user to provide a reasoned objection to the intermediary, which could then be assessed by the court (the court duly considered the user's anonymously provided objections, and finally ruled in the claimant's favour); Rb. Den Haag 5 October 2015, ECLI:NL:RBDHA:2015:11408; Rb. Den Haag 6 November 2015, ECLI:NL:RBDHA:2015:12706.

Q1.2.2: Does the proposed Directive on certain aspects concerning contracts for the supply of digital content *(COM(2015)634) provide for appropriate rules enabling the achievement of a genuine digital single market? ('DCD') & Q1.2.3: Does the proposed Directive on certain aspects concerning contracts for the* online and other distance sales of goods *(COM(2015)635) and the envisaged full harmonisation of key contractual rights provide for appropriate rules enabling the achievement of a genuine digital single market?*

In general, the maximum harmonisation approach adopted in both legislative proposals is considered an important step forward and welcomed in light of the aim to establish a digital single market. *"Given this overall aim to facilitate online shopping and the provision of digital services in the single market, anything but a maximum harmonisation would function as a restriction on this market",* the Norwegian rapporteurs note.

Nevertheless, several criticisms are being voiced in the reports.

- In Member States where existing standards of protection are high – such as in the Nordic countries – *maximum harmonisation* risks lowering the level of protection (cf. Finnish, Greek, Irish and Norwegian reports).
- The use of some *rather vague and open concepts* (e.g. 'reasonable time', 'significant inconvenience'), which would leave a wide measure of discretion to national judges, creating possible discrepancies among Member States, as well as legal uncertainty, arguably contradicts the maximum harmonisation approach (cf. Italian report).
- Several rapporteurs (Belgium, Croatia, Greece, the Netherlands, Portugal, Slovenia, Sweden...) criticise the fragmentation of the consumer protection regime that will result from the new legislative initiatives. They point to unjustified *divergences* that will be created in the legal treatment of digital content provided on a material medium ('goods') and digital content not provided on a material support ('services'), as well as to the difference in treatment that will be created between online sales and distance sales of goods, on the one hand, and other sales which remain subject to the traditional consumer goods guarantee scheme, on the other hand. Such *regulatory divergence between online and offline sales* is considered unworkable in practice and inappropriate, especially in light of the increasing importance of the omni-channel distribution model (*i.e.* selling at the same time via multiple channels such as directly in a shop, online or otherwise at a distance), or in the case of hybrid sales which combine both online and offline elements (e.g. ordering a good online and collecting it in a

brick-and-mortar shop).[52] The Belgian rapporteurs note that it would have been preferable to revise the whole system of the guarantee of consumer goods, without making any difference according to the mode of conclusion of the contract. *N.B. It should be noted that on October 31, 2017, the European Commission adopted an amended proposal on online and other distance sales of goods, extending the scope of the proposed directive to also cover offline sales and repealing the 1999 Consumer Sales and Guarantees Directive*[53] *(see the Institutional Report for more information).*

- The application of the rules in the proposed DCD to contracts for the supply of 'gratuitous' digital content is considered controversial, in particular as the proposal makes use of the notion of *'counter-performance' by way of the supply of personal data* (see in this respect e.g. the Belgian, Dutch and Greek reports which refer to further literature[54]). Some agree with the EDPS, who warned in his Opinion of 27 June 2017 that *"personal data cannot be considered as a mere commodity"*. Others are of the view that it is a good thing that such contracts are covered by the proposal, but do not welcome the fact that it would not apply if the information is not provided *actively* by the consumer (but instead gathered secretively through cookies by the supplier).
- The country reports mention some other aspects which would need further clarification, e.g. the relationship between the proposed rules and general contract law (e.g. Polish and Dutch reports); the period during which the seller is liable for lack of conformity (two-years, or longer); the enforcement of the rules (e.g. Hungarian report).

Q1.2.4: How do you evaluate the effect of the harmonised above rules on the enforcement of EU consumer protection legislation?

[52] Also the Commission itself admits that such scenario would be unfortunate (see Explanatory Memorandum to the proposed Online Sales Directive, p.3).

[53] Amended proposal for a Directive on certain aspects concerning contracts for the online and other distance sales of goods, amending Regulation (EC) No 2006/2004 of the European Parliament and of the Council and Directive 2009/22/EC of the European Parliament and of the Council and repealing Directive 1999/44/EC of the European Parliament and of the Council, 31 October 2017, COM(2017) 637 final.

[54] E.g. M.B.M. Loos, "Not good but certainly content. The proposals for European harmonisation of online and distance selling of goods and the supply of digital content", in: I. Claeys and E. Terryn (eds.), *Digital contracts*, Cambridge: Intersentia, 2017, p. 3-53 (p. 29); F. Zoll, "Personal Data as Remuneration in the Proposal for a Directive on Supply of Digital Content" and R. H. Weber, "Data Protection in the Termination of Contract", both in: R. Schulze, D. Staudenmayer, S. Lohsse (eds.), *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps – An Introduction*, 2017.

(Full) harmonisation is seen as a positive step towards the completion of the Digital Single Market, benefitting both consumers and businesses. In practice, though, there is still fragmentation of specific provisions at Member State level, since – notwithstanding the maximum harmonization character – some issues remain generally within the competence of the Member States. The Belgian rapporteurs refer, for instance, to the civil or criminal penalties that may be imposed in case of non-compliance with the rules adopted. Hence, the risk of forum shopping providers, tempted to settle in a state known for the low level of sanctions or prosecution, will remain. Several rapporteurs (e.g. Hungary, Portugal, Slovenia) emphasize the enforcement aspects and the necessity of cooperation between Member States' competent authorities (referring to the importance of the Consumer Protection Cooperation mechanism based on Regulation No. 2006/2004). In this context, it can be noted that the proposed reform of Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, is considered a step in the right direction. The possibility of a common procedure coordinated by the European Commission whenever there is a reasonable suspicion of a "widespread infringement with a Union dimension" (*i.e.* harming consumers in at least three quarters of the Member States, accounting together for at least three quarters of the EU population), is welcomed. The Italian rapporteurs note that it would be preferable to have a single, lower threshold --corresponding to three Member States-- to trigger the European Commission's coordination action (which would be coherent with the framework in place for cooperation among national competition authorities within the European Competition Network). The enforcement system should in their view also be improved by increasing the fines that national authorities may impose for an infringement of the directives (UCPD and CRD).

The obligation for Member States in the draft DCD to grant rights to certain bodies to take action before the national courts, such as national bodies, consumer organisations, or professional organisations, is referred to in the Croatian report as an important advantage for the enforcement of consumer protection law.

Q1.2.5: Do you consider the current EU consumer protection law (i.e. Unfair Commercial Practices Directive 2005/29/EC; Unfair Contract Terms Directive 1993/13/EC and Directive 2011/83/EC on Consumer Rights) appropriate for protecting consumers in their dealings with online platforms*?*

The views are mixed. Several rapporteurs (e.g. Finland, Italy, the Netherlands, Sweden) note that these Directives offer a good starting point, although they leave many gaps (like the fact that most of the existing consumer protection

rules apply only where the trader provides goods or services in exchange for money) or offer room for improvement (e.g. with regard to the right to redress and cross-border enforcement). It is also important to understand that, in many cases, the provider of the service offered on the platform will be a non-professional service provider (P2P), in which case the existing rules on consumer protection do not apply[55] (and it does not seem reasonable to extend them because no unbalance exists between peers, the Spanish report notes).

Other rapporteurs give a firm negative response, stating that existing consumer protection law does not directly or at all deal with a number of issues which are to a large extent specific to dealings undertaken with or through online platforms including data protection aspects, consumer information in the context of reliance on algorithms and the level of protection afforded by consumer protection legislation in consumer to consumer trade undertaken though online platforms (see e.g. the Irish report). As in recent years, online platforms have gained significant importance, the Slovenian report suggests that EU consumer protection law should regulate their relationship with the consumers expressly and in more detail as the current legislation so as to cover all relevant details of the relationships between consumers, online providers and traders using online platforms.[56]

Conversely, the Czech report warns that excessive and unbalanced regulation of online platforms could have adverse consequences for the provider, the user or the market itself.

Q1.2.6: Has there been any action before your national courts on the basis of consumer law against online providers' terms and conditions*?*

Various country reports describe legal actions challenging the validity of online providers' terms and conditions, albeit not always brought on the basis of consumer protection law (but on the basis of e.g. contract law) or not always started by consumers themselves (but rather by the consumer protection or competition authority, like in Hungary and Italy, or by consumer organisations, such as the Dutch *Consumentenbond* or the Swedish *Konsumentombudsmannen*).[57]

[55] At least not in the P2P or C2C relationship. In that case, the Swedish report notes, the consumer rules apply rather to the relationship between the online platform and the sellers of goods or services, since the latter qualify as "private individuals".

[56] They refer to the Discussion Draft of a Directive on Online Intermediary Platforms drafted by the Research group on the Law of Digital Services as a useful starting point: Research group on the Law of Digital Services, "Discussion draft of a Directive on online intermediary platforms", *Journal of European Consumer and Market Law*, Issue 4/2016, 164 ff.

[57] Relevant court decisions on abusive clauses in Portugal are available from an online repository maintained by the Directorate-General for Justice Policy (DGPJ) (starting in 2015): http://www.dgpj.mj.pt/DGPJ/sections/sobre-dgpj/anexos/registo-das-clausulas/

The Polish and Hungarian reports list several clauses which have been found illegal by the courts (e.g. that registration of an account in the online store amounts to acceptance of processing of personal data for marketing purposes, including sending marketing information to the site's administrator). In Hungary, such cases against websites' terms of service have been started by the National Consumer Protection Authority and the Hungarian Competition Authority (e.g. PrePayOnline case). Serious infringements were found in case the webshop or other electronic commercial service provider did not inform its consumers about some relevant company data or terms before the contract; acted against the consumers' right of withdrawal; or applied proven unfair contract terms.

The Italian Competition Authority, AGCM, has equally been quite active in recent years. It has conducted several investigations pursuant to the rules on Unfair Contract Terms and Unfair Commercial Practices, some of which have resulted in significant fines. AGCM imposed e.g. a 300,000 EUR fine on Amazon in 2016 for failing to provide (sufficient) information to consumers purchasing online; a 3 million EUR fine on Samsung in 2017 for forcing consumers – in order to benefit from a promotional price for the device they wanted to buy – to register on its platform "Samsung People" and to give consent to the use of their personal data for marketing purposes; and a 3 million EUR fine on WhatsApp in 2017 for forcing users to accept in full its new Terms of Use (and specifically the provision to share their personal data with Facebook), by inducing them to believe that – without granting such consent – they would not have been able to continue to use the service anymore.[58] AGCM is also investigating so-called "*influencer marketing*" practices carried out on social media,[59] which may violate the prohibition of surreptitious (hidden, misleading) advertising.

In France, an interesting case was brought against Facebook for its removal of access to the reproduction of the work of Gustave Courbet's 'The origin of the world'. In a judgment of 12 February 2016, the Paris Court of Appeal declared itself competent pursuant to Articles 15 and 16 of the (2001) Brussels I Regulation to rule on the lawfulness of the forum selection clause in Facebook's general conditions of use (in favour of the state and federal courts in Santa Clara County, California). The Court found that this clause, written to the detriment

[58] The 2014 decision of AGCM imposing a fine of 500,000 EUR against Tripadvisor for publishing misleading information about its reviews was overruled by the Italian Administrative Court of First Instance (the "TAR Lazio") in July 2017, holding that the type of information provided to consumers by Tripadvisor was coherent with the level of "expertise" that could reasonably be expected from an average internet user in 2014. AGCM lodged an appeal against the TAR Lazio's decision, which is still pending before the Council of State.

[59] Such practices consist of the posting on social networks of photos, videos, and comments by bloggers and influencers showing support or approval of specific brands, thus generating an advertising effect, without making clear to consumers the commercial intent of the communication.

of the consumer and creating a significant imbalance, should be regarded as unreasonable and therefore deemed to be unwritten.

Q1.2.7: Do you consider it necessary/useful to expand the scope of the rules on Business to Consumers (B2C) to Business to Business (B2B)?

The answers to this question are very divergent. Some rapporteurs, like the Dutch one, respond affirmatively and give several reasons: the fact that, in contracts with other businesses, a business may still be the weaker party and in need of protection (especially, as the Estonian and Maltese reports note, in the case of SMEs and micro-businesses); or the restrictive interpretation of the notion of consumer by the Court of Justice[60] (resulting in many cases where a natural person acts for dual purposes, *i.e.* both as a private person and in the course of a business, e.g. when buying a laptop computer, and consequently falls outside the protection of EU consumer law). Seven Member States, including Italy, have already opted (although to different extents) to apply the UCPD also to B2B relations.[61] Also the Polish and Greek rapporteurs mention that their legal systems have a unified notion of unlawful business practices which covers both acts of unfair competition (B2B) and unfair market practice (B2C), *i.e.* with unified rules for B2B and B2C.

The majority of rapporteurs, however, are not in favour of such extension, given the significant differences between B2C and B2B contexts (see e.g. the Austrian, Czech, Finnish, German, Portuguese, and Spanish reports). According to the Austrian rapporteurs, such an approach would contradict the basic values of Austrian company law, which formally delineates the demarcation for reasons of legal certainty. The German rapporteur calls the idea of extending the rules to B2B '*systemwidrig*'. Also the Spanish rapporteurs do not consider the expansion of consumer protection legislation to B2B relationships to be the solution for existing and potential conflicts between service providers and online platforms. A stricter application of competition law and maybe some provision of unfair competition might be more effective.

The Belgian and Irish rapporteurs adopt a more intermediate position. According to the former, consumer protection rules are currently justified by the presumed weakness of consumers (lack of knowledge on factual or legal aspects of the contractual relationship) when they engage with professionals. Therefore, these rules should *only* be extended to companies in their dealings

[60] See e.g. CJEU 20 January 2005, case C-464/01, ECLI:EU:C:2005:32 (Gruber/Bay Wa AG).

[61] See Guidance on the application of the Unfair Commercial Practices Directive, SWD(2016) 163 final, p. 10. As of 2016, such Member States were Austria, Sweden, Denmark, France, Germany, Italy and Belgium.

with other companies *if* it is shown that they suffer from a similar position of inferiority that justifies the existing. The view of the Irish rapporteurs goes in the same direction: although they do not consider it immediately apparent that all consumer protection rules should be extended to B2B commerce, they consider the possibility of revising the definition of consumers so that it may include SMEs ("possibly on request").

1.3. Geo-blocking

Q1.3.1. The envisaged Regulation (COM(2016) aims at preventing unjustified discrimination on the basis of a consumer's domicile or nationality in cross-border situations. How do you see the interlink between this Regulation and the Brussels I Regulation (Regulation 1215/2015) on the issue of a trader "directing activities to another Member State where the consumer has its domicile" for the purposes of determining jurisdiction?

The Geo-blocking Regulation was adopted in February 2018.[62] Most rapporteurs note that the Geo-blocking Regulation itself (Article 1(5) and recitals 9-10 in the Commission's proposal; Article 1(6) and recitals 12-13 in the final text) states that compliance with it cannot be interpreted as a sign that a professional is directing his activities to the Member State where the consumer has his habitual residence within the meaning of Article 17 of Regulation 1215/2012.[63] Following the test adopted by the CJEU, e.g. in cases C-255/08 *Pammer* and C-144/09 *Alpenhof,* all relevant elements must be taken into account in deciding, on a case-by-case basis, whether a trader has directed activities to a Member State and evidence is required demonstrating that the trader was envisaging doing business with consumers domiciled in other Member States, including the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with those consumers.

Hence, the Dutch rapporteur notes, when a trader is compliant with the Geo-blocking Regulation solely to fulfil its obligations under this Regulation, there is in principle no risk that Article 17(1)(c) Brussels I Regulation will be triggered (*i.e.* that a consumer may bring proceedings against the trader in the courts of

[62] For more information, see the Institutional Report and http://www.consilium.europa.eu/en/press/press-releases/2018/02/27/geo-blocking-council-adopts-regulation-to-remove-barriers-to-e-commerce/.

[63] The Slovenian report notes that this is especially important for traders from smaller Member States which are practically compelled to use a foreign language – often English – to conduct any cross-border operations, whereas traders from the largest Member States can use their own language to conduct business with customers from other countries.

the Member State where the consumer is domiciled). However, he continues, when a trader is being *'compliant plus'*, *i.e.* going further than is required under the Geo-blocking Regulation, there can be a debate whether the trader is directing its activities to the Member State where the consumer has its domicile. This is especially the case when, for example, the trader translates its website into the local language of the customer and/or offers delivery to the place of residence of the consumer, which is not required under the Geo-blocking Regulation (cf. recital 23). According to the Dutch report, it can be assumed in such circumstances that the trader does direct its activities to the consumer's Member State within the meaning of Article 17 (1).

The Swedish rapporteur notes, that in spite of Article 1(6) of the Geo-blocking Regulation, it is likely that traders would have to be cautious in handling transactions with consumers in Member States to which they have no intention to sell. Conversely, consumers may face difficulties in assessing whether a transaction is the result of a commercial decision by the trader or is merely imposed by the prohibition of discrimination. The Italian rapporteurs stress that national courts would have to ascertain the trader's intention to direct his activities to the Member State of the consumer's domicile on the basis of the objective factors developed in the CJEU case law, and would likely have to exclude such an intention whenever "*a trader is legally* coerced *to serve consumers in a certain state*". They see the entry into force of the Geo-blocking Regulation as an important opportunity for the CJEU to reconsider its well-established interpretation enshrined in the *Pammer* judgment.

1.4. Questions related to the collaborative economy[64]

Q1.4.1: What are the most contentious legal issues in your country raised by the collaborative economy businesses?

From the country reports, it is clear that the introduction of Uber has sparked a lively debate (and triggered numerous actions in court[65]) throughout Europe on the regulation of passenger transport services (with a driver) and on the requirements that this type of service should be subject to in the event it is mediated by an online platform. The same can be said about Airbnb. All Member States seem to be struggling with how to qualify collaborative economy businesses and whether (and to what degree) traditional sector-specific regulations, such as with

[64] The Communication adopted by the Commission on "A European agenda for the collaborative economy" (COM(2016)356 final) is discussed in the Institutional Report.

[65] In some instances resulting in the blocking of some of the Uber services, or in fines imposed on Uber drivers.

regard to taxis or housing, apply or should apply to them. Also taxation, employment issues, and consumer protection are mentioned several times as popular topics of legal debates on the sharing economy.

Some of these legal conflicts have already found their way to the CJEU, which was invited to rule on the central question whether a service such as that provided by Uber should be classified as an information society service for the purposes of the relevant provisions of EU law. In the Spanish Uber case, the Court ruled that Uber's 'intermediation service', the purpose of which is to connect, by means of a smartphone application and for remuneration, non-professional drivers using their own vehicle with persons who wish to make urban journeys, must be classified as 'a service in the field of transport' within the meaning of Article 58(1) TFEU, since it is inherently linked to a transport service.[66] Consequently, such a service falls outside the scope of Article 56 TFEU, the Services Directive and the E-Commerce Directive. Also in the French Uber case, the Advocate General took the view that Uber's activities are not to be regarded as an information society service because of their composite nature.[67] Hence, provisions of national law which apply to services such as those offered by Uber do not have to be notified as rules on services within the meaning of the provisions of EU law on technical notification (Directive 98/34, as amended).

Several Member States are in the process of, or are considering, adopting specific laws aimed at regulating collaborative economy services. Greece, for instance, adopted in December 2016 Law 4446/2016 in which it has defined sharing economy *("oikonomia tou diamoirasmou")* as *"any model where digital platforms create an open market for the temporary use of goods or services that are often provided by individuals",* and digital platforms as *"electronic, bilateral or multilateral markets where two or more user groups communicate via an internet platform to facilitate a transaction between them"*. Also in Italy, against the background of intense legal proceedings against Uber, a bill was introduced into Parliament in January 2016 aiming at regulating collaborative economy services (*Regulation of digital platforms for the sharing of goods and services and the promotion of the sharing economy).* The bill defines collaborative economy as the economy generated by the optimised and shared allocation of goods (albeit without any transfer of ownership rights) and services through digital platforms. The purpose of such legislative initiatives, like in Greece and Italy, is to create a level playing field for digital platforms offering collaborative economy services with a view to both fostering competition between innovative and traditional players and avoiding that the

[66] CJEU, Case C-434/15, *Asociación Profesional Élite Taxi v. Uber Systems Spain SL,* 20 December 2017, ECLI:EU:C:2017:981.

[67] CJEU, Case C-320/16, *Uber France,* Conclusion AG, 4 July 2017, ECLI:EU:C:2017:511.

latter are negatively impacted by the rise of disruptive technologies; to ensure a minimum level of protection for users and third parties; and c) to address the phenomenon of 'black economy' and tax evasion resulting from the absence of a regulatory framework.

With regard to the latter (taxation) aspects, the Estonian report describes – labelling it a 'success story' – how, since 2015, rideshare drivers can declare their income through a prefilled form provided by the Tax and Customs Board of Estonia. Additionally, on June 14, 2017, the Estonian Parliament passed the so-called rideshare bill, that intends to soften existing taxi service requirements and to impose equivalent rights and obligations to ride sharing services.

The Dutch rapporteur pays attention to some successful cooperative efforts towards regulation, so-called 'right to challenge' experiments, in which the public authorities allow collaborative economy businesses to propose alternatives to current regulation. The report notes how Amsterdam is generally regarded as progressive in its approach to the collaborative economy and has even been dubbed a 'sharing city' for its willingness to work with various collaborative economy platforms. Most notably, the city of Amsterdam entered into a Memorandum of Understanding ('MoU') with Airbnb, setting out common goals and rules aimed at curbing the negative effects on neighbourhoods of permanent commercial renting of apartments using Airbnb. For example, the MoU contains a rule that apartments may only be rented out for a maximum of 60 days per year.[68] The Czech rapporteurs notes that the municipality of the capital city of Prague is considering following the example of Amsterdam.

Q1.4.2: Competition issues: Does the fact that such businesses enter markets so far served by traditional service providers raise competition issues?

Several country reports (see e.g. Estonia, Spain, etc.) indicate that, depending on the sector, the collaborative economy may boost competition, increase consumer's choice, and create new markets, attracting customers who previously did not use the 'traditional' services (because the price was too high, or the service was not user-friendly, etc.). A market study in Estonia, for instance, showed a positive effect on the financial market, where the sharing economy platforms address foremost a target group whose needs are not satisfied by commercial

[68] Memorandum of Understanding between city of Amsterdam and Airbnb available at: https://www.amsterdam.nl/publish/pages/813509/agreement_amsterdam_and_airbnb_mou.pdf. As testimony to the success of this cooperation, the European Commission considers the MoU to be a 'best practice' in developing an EU-wide model contract for use by municipal authorities and home sharing services.

banks.[69] However, as the Swedish rapporteur notes, the emergence of online platforms also puts a significant pressure on traditional businesses in a number of sectors (in the hotel industry, taxi transport, meals and catering...).

The country reports describe two types of competition issues arising from the entry of collaborative economy businesses (see e.g. the Czech, Finnish, Irish, Italian and Spanish reports). On the one hand, rapporteurs mention ongoing discussions over an alleged lack of 'level playing field' (whereby newcomers are being accused of engaging in 'unfair competition' with traditional service providers by not respecting existing regulations on employment, health, safety etc., whereas the newcomers argue that those regulations do not apply to them – national courts are adopting diverging views on this issue). On the other hand, they note that new anti-competitive practices are emerging (such as the coordination of behaviour, or even price fixing) as a combination of the platform and user actions, and/or as a result of machine learning technologies, for which, at first sight, neither individual users, nor the platform provider might be liable.

Several country reports (France, Greece, Italy...) refer to the investigations carried out by their national competition authorities into online travel agents' (OTA) parity clauses (or 'Most Favoured Nation' clauses). Following a complaint from the major French hotel unions and the Accor group, the French Competition Authority started an investigation in the online hotel booking sector. In April 2015, Booking.com committed to change its 'wide' parity clause to a 'narrow' parity clause.[70] The Italian and Swedish Competition Authorities pursued a similar commitments approach, whereas Germany's Bundeskartellamt has pursued a prohibition approach. In December 2015, it prohibited Booking.com's narrow parity clause in Germany. In the context of the European Competition Network, a group of eleven EU competition authorities (including the Belgian, Czech, French, German, Hungarian, Irish, Italian, Dutch, Swedish and UK national competition authorities and DG Competition) carried out a coordinated monitoring exercise in the online hotel booking sector in 2016.[71] In addition to these antitrust measures, legislators in e.g. France and Austria have intervened to render null and void all OTA price parity clauses (through the so-called *Loi Macron* in August 2015, respectively, through an amendment to the Austrian law on unfair

[69] Technopolis Group study on the sharing economy in Estonia, available in Estonian, executive summary available in English: https://www.mkm.ee/sites/default/files/lopparuanne.pdf

[70] A 'wide' parity clause oblige the hotel to give Booking.com the lowest room prices and best room availability relative to all other sales channels, whereas a 'narrow' parity clause allow the hotel to offer lower room prices and better room availability on other online travel agents' platforms and on offline sales channels, but allow Booking.com to stop the hotel from publishing lower room prices on the hotel's own website.

[71] The report was published in April 2017; http://ec.europa.eu/competition/ecn/hotel_monitoring_report_en.pdf

competition in November 2016).[72] Also the Swiss Parliament recently adopted a motion inviting the Federal Council to submit the necessary legislative amendments for the prohibition of tariff parity clauses in the contractual relationship between hotels and online booking platforms.[73]

The Portuguese rapporteurs refer to a report that was published in December 2016 by their National Competition Authority ('AdC') on competition and regulation in passenger transport services.[74] It is based on a public consultation and analyses the constraints that existing rules pose to competition in this market. Limitations such as quantitative restrictions on the number of operators or the administrative setting of prices[75] were heavily criticised by the AdC for being disproportionate and harmful to competition. As a result, the AdC recommended that the Government reassess the current quantitative restrictions and price setting regulations for taxis, with the explicit recommendation that the new rules should not extend heavy regulation to new entrants but merely establish a level playing field. At the time of closing the Portuguese report, the debate on regulatory reform was still ongoing.

In a recent report on the collaborative economy, the Swedish Competition Authority *(Konkurrensverket)* noted that current competition rules are generally *"well suited to deal with competition-related problems that may occur with these new services"*, but it suggested at the same time introducing new thresholds for merger control as the turnover of e.g. online platforms at the time of such transactions does not necessarily reflect their market power (see, in this regard, also the Swiss report).[76]

As a side note, reference can be made to the German Federal Cartel Office's *(Bundeskartellamt)* preliminary assessment of 19 December 2017 in its proceedings against Facebook.[77] The *Bundeskartellamt* considers that Facebook abuses its dominant position through imposing unfair general terms and conditions

[72] See the aforementioned monitoring report, p.4-5.

[73] Motion 16.3902, Pirmin Bischof, Verbot von Knebelverträgen der Online-Buchungsplattformen gegen die Hotellerie / Interdire les contrats léonins des plates-formes de réservation en ligne dont l'hôtellerie fait les frais, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163902

[74] Press release available at http://www.concorrencia.pt/vEN/News_Events/Comunicados/Pages/PressRelease_2016.aspx?lst=1&Cat=2016.

[75] Taxi tariffs in Portugal are set by conventions between the Directorate-General for Economic Activities and associations representing the taxi license holders.

[76] Swedish Competition Authority (2017:2) "*Konkurrens och tillväxt på digitala marknader – ett regeringsuppdrag om e-handel och delningsekonomi*" (1 March 2017).

[77] The Preliminary Assessment and a background paper are available from: http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html?nn=3591286. For a commentary, see e.g.: http://competitionlawblog.kluwercompetitionlaw.com/2018/01/09/bundeskartellamt-sends-preliminary-assessment-facebook/ .

on its users: by making the use of its social network conditional on its being allowed to limitlessly amass every kind of data generated by using third-party websites and merge it with the user's Facebook account, Facebook is imposing terms of service which are inappropriate and violate data protection provisions to the disadvantage of its users. Although this case is not directly related to the discussions about the collaborative economy, it triggers interesting questions to what extent violations of consumer protection or data protection rules may constitute an abuse of dominance. According to Andreas Mundt, the President of the *Bundeskartellamt, "[d]ata protection, consumer protection and the protection of competition interlink where data, as in Facebook's case, are a crucial factor for the economic dominance of a company."*[78]

Q1.4.3: Market access requirements: What kind of service providers active in the collaborative economy are required to obtain authorisations under national law in your country and under what conditions can such authorisations be obtained? Are the relevant administrative procedures and formalities clear and transparent?

Market access requirements relevant for collaborative economy service providers usually apply in relation to passenger transport, apartment rentals and hospitality business (meals and catering). The first category often entails the acquisition of a taxi driver's license (with a limited number of such permits being available), the keeping of records on transported persons, and safety requirements. The second category mainly consists of hygienic and safety regulations, as well as (city) tax duties, and notification of accommodated guests. The third category relates to food safety requirements.

In various countries (e.g. Czech Republic), it is still unclear – due to pending final court decisions – to what extent these requirements apply to e.g. Uber drivers. Other country reports note that some of these requirements (especially the traditional limitation of available taxi licenses, but also new regional rules imposing minimum stays on short-term rentals) are being challenged by National Competition Authorities because of their anti-competitive effect (see e.g. the Spanish report).

Some countries (like Finland and Portugal) have adapted, or are in the process of adapting, their laws to take into account service providers in the collaborative economy, mainly in the area of passenger transportation services and for short-term rentals.[79]

[78] See Preliminary Assessment of 19 December 2017, mentioned in the previous footnote.

[79] The new Finnish Act on Transport Services, which will enter into force in July 2018, quashes the current system of limited number of taxi permits.

Q1.4.4: Consumer protection: Are consumer protection issues the subject of legal challenges in your country? & Q1.4.5: Under which conditions in a peer-to-peer provision of services the provider of the underlying service qualifies as a trader according to your national law?

The Italian report highlights how the collaborative economy has blurred the distinction between traders and consumers since products and services are increasingly offered by subjects which act in their capacity as consumers and not traders or, in some cases, these services are directly offered by consumers to traders. This switch, from B2C to C2C (or in some cases C2B), raises difficulties in clearly determining the scope of consumer law.

National definitions of 'trader' are usually aligned with the definition of the term in EU consumer law (see e.g. article 2(b) UCPD: *"'trader' means any natural or legal person who [...] is acting for purposes relating to his trade, business, craft or profession and anyone acting in the name of or on behalf of a trader"* – idem article 2(2) Consumer Rights Directive) and, hence, do not explicitly specify whether this includes or excludes the concept of P2P service provision. When a peer-to-peer provider of an underlying service should qualify as a trader must be assessed on a case-by-case basis. This may involve factors such as the regularity with which a person provides services or sells goods on P2P platforms (excluding merely occasional offers), revenue thresholds or what proportion of that provider's overall income is derived from these activities. Therefore, an individual which intermittently provides services or sells goods to other individuals is, generally speaking, not considered a trader under consumer protection legislation. By contrast, when providing a P2P service a person is acting for purposes related to his trade, business or profession, he will be considered a trader.

The Swedish report mentions a recent Government-commissioned report which examined the concept of 'trader' within the context of the collaborative economy.[80] It stated that the concept covers *"all physical or legal persons who run an economic operation of a certain size and duration and of such character that it may be designed as professional"* (p.39) and that, given this elastic definition, a case-by-case assessment is required in order to assess whether a supplier of goods or services qualifies as a trader. The report did not propose legislative changes to clarify this issue, but noted that the extent of the problem was still limited given the novelty of this phenomenon. It rather called for a regular overview of the collaborative economy and proposed that the Swedish Consumer Agency (*Konsumentverket*) be tasked with providing independent information and guidance on e.g. the legal status of users involved in the collaborative economy.

[80] Government-commissioned report (2017:26) "*Delningsekonomi – På användarnas villkor*" (March 2017).

Q1.4.6: How can legal rules contribute to remedying the lack of consumer confidence in peer-to-peer services? Do you think that trust-building mechanisms such as online rating and review systems and quality labels are appropriate tools to overcome the lack of information about individual service providers? What other tools would you consider appropriate?

The general feeling amongst country rapporteurs is that online ratings and reviews can be appropriate tools as they enhance transparency and help to overcome the problem of information asymmetry, but that there is also scope for caution: firstly, because they can be easily manipulated (see e.g. the Spanish report); secondly, because the implementation of such rating and reviewing systems may create the perception that digital platforms exercise editorial responsibility over the content of reviews, which might exclude them from the liability exemptions in the E-Commerce Directive (see e.g. the Italian report); and thirdly, because they might impede market access to newcomers (*i.e.* service providers or consumers who have not accessed the platform before and therefore do not currently have any rating, creating room for distrust) (see e.g. the Estonian report).

The Spanish rapporteurs refer to other instruments that can increase trust and security, such as (i) the control of the identity of the parties in the platform (provision of some kind of ID); (ii) the control of minimum quality features of the service providers (e.g. a driver's license for providers of transportation services); (iii) the provision of insurance; and (iv) management of payments for the parties. Here again, it is noted that such instruments entail the risk of backfiring, when they would be considered as evidence of the fact that platforms are not merely intermediating but actually providing the underlying service. It is therefore considered important to give certainty to the platforms themselves, as to ensure that such a provision does not entail that the underlying service is the responsibility of the online platform.

Also the French report (under Q1.1.1 and Q1.1.2) describes alternative measures that could be adopted with regard to the collaborative economy. It refers to the annual study of the State Council of 2017, entitled *"Public Power and Digital Platforms: Supporting the uberisation"*, which suggested a balanced set of complementary measures at European level, but also at national level: *on the one hand*, rules for platforms with regard to loyalty and responsibility in the use of algorithms, as well as rules ensuring tax and social fairness between the traditional economy and the digital economy; *on the other hand*, the promotion of an environment conducive to the development of platforms, by supporting individual entrepreneurship, administrative simplification for platform collaborators,

and systematic impact studies of new regulations regarding their effects on the 'agile' economy.[81]

It is mentioned several times in the country reports that authorities should refrain from overregulating. To use the words of the Slovenian rapporteurs: *"collaborative economy markets should remain as open and non-regulated [as possible]"*. It is therefore generally considered more suitable to rely on self-regulatory mechanisms, rahter than to impose the implementation of rating and reviewing systems through legal obligations. The Ecommerce Europe Trustmark is named by the Czech rapporteurs as an example. Another example comes from Portugal, where the Portuguese Consumer Protection Association (DECO), together with the Digital Economy Association (ACEPI) and the DNS.PT association, have designed an accreditation mechanism that online e-commerce platforms in general may sign up to in order to benefit from a quality certification under the Confio ("Trust") stamp.[82]

2. Digital media

Like other goods and services, the audiovisual media are subject to the rules of the single European market. The media sector is facing a major transformation as a result of digitisation, the rise of the Internet and convergence[83] between print and audiovisual media, on the one hand, and between traditional and social media, on the other hand. These days we can watch our favourite programmes from all over Europe not just on TV, but also via the internet or on our mobile devices. Publishers of online newspapers and magazines increasingly offer clips on their websites as an add-on to written articles. Frequently, these clips are compiled in separate spaces of the websites with particular navigation tools for users (such as most recent videos, most watched videos), and they may cover the entire range of subjects reported on. Whereas users may not consider the origin of those videos (newspapers, broadcaster, other) as particularly relevant, the distinction between press products and audiovisual media services is crucial from a legal perspective as different legal requirements and regulatory regimes apply. Publishers of newspapers, in printed form or online, are subject to a much lighter set of statutory rules (being predominantly subject to self-regulation only) compared to audiovisual media services which are regulated by the EU's Audiovisual

[81] In its communication "A Fair and Efficient Tax System in the European Union for the Digital Single Market" of September 21, 2017, the European Commission proposed a number of short-term options for tax fairness.

[82] They have also approved a voluntary code of conduct (Confio.pt), in accordance with Article 16 of the E-Commerce Directive, which is available at https://www.confio.pt/o-confio/codigo-de-conduta/.

[83] Convergence refers to the blurring of formerly distinct boundaries between two markets or two media genres.

Media Services Directive (AVMSD). The AVMSD governs EU-wide coordination of national legislation on all audiovisual media, both traditional TV broadcasts and – since 2007 – on-demand services. The AVMSD is currently under review; a new legislative proposal amending the AVMSD has been adopted by the European Commission on 25 May 2016.

At the same time, and also in the context of its Digital Single Market Strategy, the Commission is rolling out an ambitious modernisation of the EU copyright framework.[84] The objective is to make EU copyright rules fit for the digital age. The Commission published a Communication on a modern and more European copyright framework on 9 December 2015, together with a draft Regulation on ensuring the cross-border portability of online content services in the internal market, which was adopted in 2017. The Regulation aims to ensure that consumers who buy or subscribe to films, sport broadcasts, music, e-books and games can access them when they travel in other EU countries.

A second set of legislative proposals was adopted in September 2016, and focus on allowing for wider online availability of content across the EU, adapting exceptions and limitations to the digital world, and achieving a well-functioning copyright market place. The package contains a draft Regulation which introduces the application of the country of origin to some online transmissions of broadcasting organisations, and the collective management of rights to retransmissions by means equivalent to cable (extending the specific regime for copyright licensing for TV and radio broadcasting by satellite and cable pursuant to Directive 93/83/EEC with a view to facilitating access to more television and radio programmes online from other EU countries).

2.1. Media convergence

Q2.1: In its judgment of 21 October 2015 in New Media Online GmbH v Bundeskommunikationssenat (case C-347/14),[85] the CJEU held that the concept of 'programme', within the meaning of Article 1(1)(b) of the AVMS Directive, must be interpreted as including, under the subdomain of a website of a newspaper, the provision of videos of short duration consisting of local news bulletins, sports and entertainment clips. It held that online newspapers are not per se excluded from the

[84] For more information, see the Institutional Report; https://ec.europa.eu/digital-single-market/en/copyright; and https://ec.europa.eu/digital-single-market/en/modernisation-eu-copyright-rules.

[85] Link to the judgment: http://curia.europa.eu/juris/liste.jsf?num=C-347/14 and the press release: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150127en.pdf . For a commentary, see e.g. https://www.ebu.ch/files/live/sites/ebu/files/News/2015/10/Case%20note%20New%20Media%20Online.pdf

scope of the AVMSD. If publishers offer audio-visual material they may be covered by the Directive, provided that the principal purpose test is met.[86]
Is your national practice in line with this judgment? If not, where does (or did) it deviate? Did the judgment of the CJEU lead to a different approach in your country?

According to the country reports, the large majority of Member States has transposed the definition of 'AVMS' and 'programme' in their national law in accordance with the AVMSD. Only minor differences were reported, e.g. by the French, Spanish and Dutch rapporteurs, who stressed that the national law does not really deviate from the EU position, or is interpreted in practice in conformity with EU law. The fact that the Spanish General Audiovisual Communications Act (GACA) does not explicitly refer to the comparability criterion in its definition of 'television programme', did not, for instance, prevent the Spanish media regulator (CNMC) to rely expressly on the interpretation of 'programme' given by the CJEU in the *New Media Online* case (where the importance of the comparability criterion was highlighted) when applying the GACA.

Also national practice seems to be largely aligned with the AVMSD and the CJEU's interpretation in *New Media Online*.[87] Most rapporteurs noted that, so far, neither the media regulator, nor the courts have had to deal with the matter (as is the case in Croatia, Ireland, Italy, Greece, Poland, Portugal, Romania and Norway), or that the jurisprudence is fully compatible with the Court's ruling. The Swedish and Hungarian rapporteurs describe a number of cases (some pre-dating the *New Media Online* ruling) in which the competent media authority found that the provision of on-demand videos under the subdomain of a newspaper's website qualified as an audiovisual media service, since the videos could be considered as a catalogue available separately from the textual content, rather than

[86] In a recent judgment, the CJEU ruled that the definition of 'audiovisual media service' in the AVMSD covers neither a video channel on which internet users can view short promotional videos for new passenger car models, nor a single video of that kind considered in isolation; CJEU, Case C-132/17, Peugeot Deutschland, 21 February 2018, ECLI:EU:C:2018:85.

[87] Only the Maltese rapporteur noted that national practice is presumably not in line with the CJEU ruling. It can be noted that the UK regulator Ofcom has adopted a strict interpretation of the notion 'principal purpose' and 'TV-like' and has overruled various ATVOD determinations qualifying video sections of newspapers or magazines as on-demand programme services (e.g. Sun Video; Elle TV; Vice Video cases). See: J.M. Weinand (Metzdorf), *Implementing the EU Audiovisual Services Directive – Selected Issues in the Regulation of AVMS by National Media Authorities in France, Germany and the UK; PhD thesis (promoter M. cole), University of Luxembourg*, 2016 (published by Nomos in 2018); J.M. Metzdorf (Weinand), "The Implementation of the Audiovisual Media Services Directive by National Regulatory Authorities – National Responses to Regulatory Challenges", *JIPITEC* 2014, Vol.5, No.2, p.88-104; http://www.jipitec.eu/issues/jipitec-5-2-2014/3998.

serving to supplement and illustrate that textual content. The same approach is adopted by the media regulators in Belgium.[88]

Some rapporteurs stressed the importance of codifying the CJEU's position on the occasion of the revision of the AVMSD in order to ensure consistency and remove any remaining legal uncertainty (cf. French report) or to tackle the fundamental issues resulting from growing convergence between classical opinion-forming mass media, hybrid content like information portals, and purely private content, such as on Youtube or Facebook (cf. German report).

2.2. Video platforms

Q2.2: The legislative proposal to amend the AVMS directive brings video platforms (such as YouTube) under the scope of the AVMS rules. Do you consider this a step in the right direction? How far should the extension of the scope of application towards such platforms go: only for the rules on protection of minors and the combatting of hate speech, or also for the rules on commercial communications (product placement, sponsoring, advertising...)? Does your national legislation already provide for sector-specific rules for audio-visual platforms?

The proposed inclusion of video-sharing platforms (including certain non-EU ones) in the scope of the AVMSD is one of the most contentious issues in the discussions between the European Parliament, the Council and the Commission. The lack of consensus on the definition of a video-sharing platform (does it also include social media or not?), the requirements for such platforms (only relating to the protection of minors and combatting of hate speech; or also rules on commercial communications and on media literacy?), and the flexibility for Member States to impose stricter rules (minimum or maximum harmonisation?) also transpires from the country reports.

Currently, none of the countries covered in the reports have included in the scope of their audiovisual media laws video-sharing platforms that do not exercise editorial responsibility over the content offered. Some rapporteurs note that such platforms are, however, covered under other specific or general laws (such as the German *Telemedia Act* which transposes the E-Commerce Directive and covers electronic information and communications services, to the extent they are not telecommunications or broadcasting services; the Swedish *Act on Responsibility for Electronic Bulletin Boards*; or the *French Law No. 2016-1321 of*

[88] See, for instance, the guidance issued by the *Conseil Supérieur de l'Audiovisuel* in its Recommandation relative au périmètre de la régulation des services de médias audiovisuels, March 2012, available from http://csa.be/breves/652.

October 7, 2016 on the Digital Republic). The Hungarian E-Commerce Act has installed a notice and takedown procedure (which can be triggered by minors or their legal representatives) for the removal of online content that violates the personality rights of minors (comparable to the procedure in the case of online copyright infringements), and also puts Internet service providers under a duty to show prior warnings and to place identifiers in the source code of the subpage (allowing child protection filtering software to filter out harmful content and to make it inaccessible) when their site contains content that may seriously damage the intellectual, psychological, moral or physical development of minors.

Although the platforms may have stayed out of the reach of media regulations so far, the situation is different for the providers of the content on those platforms (such as vloggers or providers of YouTube channels). The Austrian rapporteur, for instance, refers to the recent information campaign *"Dos and Don'ts on YouTube – Influencers between Business, Storytelling and Legal Framework"* launched by the media authority KommAustria and the media department of the Broadcasting and Telecom Regulatory GmbH (RTR), explaining when a YouTube channel qualifies as an on-demand media service and has to comply with the relevant reporting, labeling and regulatory obligations.[89] In France, the media regulator (*Conseil Supérieur de l'Audiovisuel)* adopted in November 2016 (for the first time) a decision against the YouTube channel *"Les Recettes pompettes by Poulpe"* (qualifying the editor Studio Bagel Productions as the media service provider subject to the rules on AVMS). The CSA found that the first episode contained propaganda in favour of alcohol in violation of the provisions of Article L.3323-2 of the public health code (many references to alcohol; presentation of alcohol likely to encourage the public to its consumption) and issued a 'warning'.

The country reports received are (with the exception of Sweden and Slovenia) unanimous in expressing support for the proposal to include new players offering audiovisual content via the internet, particularly *video-sharing UGC platforms* in the scope of the AVMSD, given that viewers increasingly access audiovisual content (including user-generated) on-demand and on connected devices, and that new online players (in particular video on-demand providers and video-sharing platforms) increasingly compete with broadcasters. The extension is considered "a step in the right direction" and is predominantly justified by the rapporteurs on the basis of the argument of ensuring a level playing field. Harmonisation at EU level is welcomed, as a fragmented regulatory framework at the national or local level would only create uncertainties for users and providers, thus undermining the functioning of the digital single market.

[89] http://www.horizont.at/home/news/detail/kommaustria-und-rtr-nehmen-youtube-ins-visier.html

The views are less aligned when it comes to the inclusion of *social media* in the definition of video-sharing platform. The Hungarian rapporteur mentions social media as playing an increasing role in informing the public, sharing information, entertaining, and publishing audio-visual content, thereby competing for the same audience and income as radio and television media services. He therefore considers the extension of EU media regulation, or at least part of it, to include social media as "completely justified", bearing in mind the rapidly changing media consumption habits and the widespread use of social media, mainly among young people. By contrast, the Swedish rapporteur notes that Sweden has in general been critical of the European Commission's proposal to bring video platforms under the scope of the AVMS Directive because of potential chilling effects on freedom of expression and of information and on an open and free internet. In particular, it has called for a clear and restrictive definition of the concept of 'video-sharing platforms' to be included and has voiced strong criticism on the subsequent broadening of the definition video platforms to include social media services *"if the proportion of audiovisual content is significant to the main activity or other activities of that service"*. Together with six other Member States, Sweden sent an unpublished non-paper to the EU Council presidency stressing the problem of requiring platforms to 'police' non-illegal content over which they do not have editorial control.[90] Rather than extending the AVMSD – which has always targeted media service providers *with* editorial responsibility – to video portals *without* editorial responsibility, the Swedish rapporteur suggests a horizontal approach to tackle problems related to e.g. online hate speech. Such horizontal approach, as outlined in the Commission's recent Communication on Tackling Illegal Content Online,[91] would have the merit of weighing in conflicting interests such as the freedom of speech and the fight against illegal content by taking into account the role(s) of intermediaries in a technologically-neutral way.

Also those rapporteurs endorsing the extension caution against **over-regulation**, as a disproportionate burden on providers could potentially affect diversity of online media, erode freedom of speech and undermine the competitiveness of European providers (cf. Estonian report). Increased oversight also comes with increased administrative burdens and, hence, increased costs, the Polish rapporteur notes. The Italian rapporteur advocates for the application of a strict necessity and proportionality assessment of the regulatory constraints on undertakings. Several others argue that an adequate balance should be sought between protecting those potentially affected and the level of regulatory intervention.

[90] According to European Digital Rights "AVMS Directive: It isn't censorship if the content is mostly legal, right?" (27 April 2017), available on www.edri.org.

[91] European Commission, Communication 'Tackling Illegal Content Online – Towards an Enhanced Responsibility of Online Platforms', 28 September 2017, COM(2017) 555 final.

The German and Austrian rapporteurs stress the need to take into account the particularities of the media used and the different provider and user structure: video platforms (such as YouTube) differ from traditional program providers in that the majority of content is created and uploaded by users. Greater regulation of these platforms is to be viewed critically, as such is accompanied by the obligation to implement preventative filtering mechanisms for content recognition. This might raise concerns about *censorship*, especially as increased platforms' responsibility also creates incentives to block the content provided by users. In addition, the Austrian rapporteur notes, this might possibly contradict the currently applicable liability exemptions in the E-Commerce Directive, notably Article 15, according to which hosting platforms must not be subject to general monitoring obligations (see above, Q1.1.3 and Q1.1.4). The French rapporteur lists a series of issues that should be clarified when extending the rules to video platforms (such as: what are the relevant levels and modes of regulation? What is the precise scope of the obligations incumbent on these new operators?).

The country reports are in agreement in finding that the extension of the rules on *protection of minors* and the combatting of *hate speech* to video-sharing platforms (as proposed by the European Commission) can be considered as a sensible legislative proposal, which presents an adequate measure for reaching the intended goal without unreasonably burdening any of the affected parties.

However, the rapporteurs express opposing views in relation to the extension of the rules on *product placement, sponsoring, and advertising.* The Spanish and Maltese rapporteurs doubt the feasibility since UGC platforms usually do not have an editorial responsibility for the content stored in the platform, and the Czech rapporteurs clearly state that, in their view, *"the current state of vlogging does not justify an extension of the scope of application for the rules on commercial communications".* The Belgian rapporteur considers that the imposition of obligations other than those relating to the protection of minors and hate speech entails an increased risk for freedom of expression and information of Internet users.

By contrast, the Hungarian country report welcomes the idea that the EU authorities should enforce certain commercial communication-related rules vis-á-vis video-sharing platforms. The report argues that the transformation of media consumption and usage habits resulted in a growing proportion of advertising spend going to online media, and in particular to the social media segment. The enforcement of certain minimum regulations on advertising, sponsorship and product placement would serve not only the interests of consumers but also the interests of economic operators active in the advertising market, by creating a predictable, fair and equal market situation for them. This view is shared by the Portuguese rapporteur.

Also the German rapporteur considers it 'vital' that consumers can distinguish between advertising communication and editorial content, across all media (hence, including on video-sharing platforms) and that a level playing field with traditional providers of audio-visual services is ensured. Since also other regulatory instruments could be used to strike such balance between consumer protection and competitiveness (e.g. unfair competition rules), he highlights the importance of coordination (an argument also put forward by the Romanian rapporteur).

2.3. Country of Origin

Q2.3: One of the major areas of debate in the context of the AVMS revision, concerns the country-of-origin principle and the criteria for jurisdiction. Have there been any disputes in your country concerning the application of the country-of-origin principle (whereby the media regulator attempted to impose certain rules on audio-visual media service providers established in other Member States)? Have there been any problems regarding providers established outside the EU and targeting your national audience?

The large majority of rapporteurs (from Austria, Czech Republic, Germany,[92] Spain, Croatia, Ireland, Italy, Greece, Malta, Poland, Portugal and Romania) indicate that there have been no (major) conflicts with the country-of-origin principle in their country, although some express criticism of the existing (or proposed, see below) anti-circumvention mechanism. The Polish rapporteur, for instance, highlights that the Polish law contains vague terms, such as "morality" or "Christian values" as standards required for all broadcasting programmes, which may render an even streamlined and well-designed procedure prone to legal ambiguity.

Jurisdiction conflicts will especially arise in situations where Member States have adopted stricter rules in areas harmonised by the AVMSD, such as protection of minors, hate speech or advertising (which is explicitly allowed by the AVMSD but those rules can only be imposed on domestic media service providers). In Sweden, for instance, broadcasting rules on alcohol are stricter than in most Member States, whereas in Norway, advertising for alcoholic beverages is entirely prohibited (as well as advertising specifically directed at children).

[92] See, however, the legal dispute between Germany and two Danish companies, *Mesopotamia Broadcast* and *Roj TV,* concerning the prohibition of their activities on account of the nature of the television broadcasts produced by those companies (amounting to incitement to hatred, according to the German authorities), which led to a preliminary ruling by the CJEU in Joined cases C-244/10 and C-245/10, *Mesopotamia Broadcast A/S METV and Roj TV v. Bundesrepublik Deutschland*, 22 September 2011, ECLI:EU:C:2011:607.

Member States may also adopt specific rules for cultural policy reasons outside the harmonised areas (e.g. the obligation for broadcasters to contribute to the national film fund). France, for instance, has developed an extensive legislative and regulatory arsenal aimed at fostering cultural diversity and supporting audiovisual creation, which providers may be tempted to escape by establishing themselves in other Member States.

A number of media authorities started procedures against media service providers established abroad (often the UK or Luxembourg), for infringement of their national rules on protection of minors (e.g. Hungary), alcohol advertising (e.g. Sweden, resulting in the *De Agostini* ruling of the CJEU), children's advertising (e.g. Norway, resulting in the *Lego/Mattel* ruling of the EFTA Court, which reached the opposite conclusion as the CJEU in *De Agostini*), incitement to hatred (e.g. Estonia), or general circumvention of the rules (e.g. Belgium, resulting in the *VT4* and *RTL Belgium* rulings of the CJEU).[93] Such action consists of either sending a request to the media authority of the transmitting state, or directly invoking the national rules against the foreign media service provider (cf. Belgian and Hungarian reports). However, of the jurisdiction conflicts described in several country reports (see in particular the Belgian, Hungarian, Estonian, Dutch, Spanish and Swedish reports), only a few cases resulted in actual remedies adopted against the broadcaster concerned for breach of the rules of the receiving state. Depending on the perspective you take, this can be considered a success in terms of the freedom to provide broadcasting services (with broadcasters being able to continue the distribution in the receiving states of their programmes which were considered in compliance with domestic law, albeit not with the receiving country's law), or as a failure in terms of protecting specific national values (resulting in 'double standards' for domestic and non-domestic broadcasters, the former being subject to the more stringent rules of their home country while competing with the latter for the same audience). A common element that transpires from the cases discussed, is the complex and time-consuming nature of the procedures involved. Although the Estonian rapporteurs refer to the excellent cooperation of the UK regulator, Ofcom, with the Estonian Technical Surveillance Authority in the case against *REN TV*, cooperation between regulatory authorities from different Member States apparently does not always follow a smooth path. The Hungarian rapporteur makes note of several cases in which the foreign authorities did not even respond to requests made by the Media Council. Also the dialogue between the Belgian *Conseil Supérieur*

[93] CJEU, Case C-56/96, *VT4 Ltd v Vlaamse Gemeenschap*, 5 June 1997, *ECR* 1997, p.I-03143; CJEU, Case C-517/09, *RTL Belgium SA*, 22 December 2010, ECLI:EU:C:2010:821. In the latter case, the Court ruled that the Belgian *Conseil Supérieur de l'Audiovisuel* could not be considered a court or tribunal in the sense of Article 267 TFEU and that the Court therefore did not have jurisdiction to answer the question referred.

de l'Audiovisuel and its Luxembourg colleagues of ALIA with a view of remedying conflicts arising from the fact that the most popular commercial station in Wallonia, RTL Group, is established in Luxembourg, has been more successful in certain periods than in others.[94]

Although the French report does not refer to specific conflicts, it stresses the importance that France has traditionally attached to combatting forum shopping, which engenders risks of unfair competition and which undermines the effectiveness of the French audiovisual rules. It considers the current anti-circumvention mechanism in the AVMSD (Article 4.2) – which is complex to implement in practice and only applies to linear services – insufficient to tackle undesired effects of the country-of-origin principle. France has extended in its national audiovisual law the scope of the anti-circumvention mechanism to cover also on-demand services (although the rapporteurs question the effectiveness of the mechanism, which has never been put to practice) and has in recent years imposed taxes on VOD operators and video platforms established outside France but addressing the French public (known as the 'Netflix tax', resp. 'YouTube tax'). The changes introduced in the legislative proposal to amend the AVMSD -- allowing Member States to require providers of on-demand audiovisual media services, targeting audiences in their territories, but established in other Member States, to make financial contributions to the production of European works (via direct investment in content or contributions to national funds) -- are welcomed by the French rapporteurs, but are not sufficiently ambitious in their view. This view is, according to the Polish rapporteur, shared by the Polish National Broadcasting Council. Also the Romanian rapporteur describes some points of criticism expressed by the Romanian National Audiovisual Council.

2.4. Media Regulator's Independence

Q2.4: The AVMS Directive today does not impose any independence or other requirements for media regulators – in stark contrast with what is the case in e.g. the telecommunications or energy sector, or for data protection authorities. Would you consider the introduction of such independence requirements for media regulators at EU level a step forward? Would it facilitate the creation of a single market for audiovisual media services? Are there any national legal obstacles to such independence requirements for media regulators? Have there been any problems of undue political or commercial pressure on media regulators in your country?

[94] The Belgian country report notes that an agreement was reached in 2010 between CSA and ALIA, but that a recent change of position by the CSA – considering it has direct jurisdiction over certain channels of RTL Group – has put the agreement under pressure.

The independence of media regulators is generally understood as the ability to take decisions autonomously, in light of the objectives set by law, free from the influence of both elected officials and private parties (in particular market actors but also user organisations). As the Dutch rapporteurs highlight, the media regulator's independence is considered crucial in ensuring that media actors comply with the rules and to protect the integrity and independence of the media landscape. *"Being the essential wall between politics and independent media, it is seen as one of the cornerstones of democracy."* Despite the fact that no stringent requirements on regulator's independence are being imposed by the AVMSD -- contrary to what is the case in the EU legislation on e.g. electronic communications networks and services, or on data protection – nearly all country reports claim that their media authority is set up as an independent regulator, in some cases pursuant to explicit and direct constitutional requirements (like in Malta, Poland and Sweden). Several rapporteurs, including the Belgian, Maltese and Polish experts, add some nuance to that observation for various reasons (e.g. because of the way in which members are being appointed by government, or because of the methods through which the regulator is financed).[95]

As the Spanish rapporteurs note, there is a broad consensus in favour of enshrining independence requirements for media regulators in EU legislation. The importance of independence for the effectiveness of regulatory oversight in the interests of citizens and consumers, as well as the sector itself, has also been highlighted by ERGA, the European Regulators Group for Audiovisual Media Services.[96] To illustrate the importance of having an explicit legal basis in EU law for the independence of media regulators, specifying the requirements of competence, independence, impartiality and transparency, the Spanish rapporteurs refer to the *Ormaetxea and Lorenzo* judgment of the CJEU of 2016.[97] In that case, two former members of the telecoms regulator which had been dismissed before the expiry of their term of office because of the creation of a new single unified authority 'CNMC' (merging several sector regulators together with the national competition authority) successfully argued that this was a breach of the independence requirements in Directive 2002/21/EC on a common regulatory

[95] In 2010-2011, a major study was carried out by an academic consortium (Hans-Bredow-Institute, KU Leuven-ICRI, CEU-CMCS, Cullen International) on behalf of the European Commission into the institutional, legal and regulatory framework governing the regulatory bodies competent for audiovisual media services in EU Member States and candidate countries, the so-called INDIREG study (Indicators for independence and efficient functioning of audiovisual media services regulatory bodies), available from http://indireg.eu/. An update followed in 2015 through the RADAR study carried out by EMR; https://ec.europa.eu/digital-single-market/en/news/study-audiovisual-media-services.

[96] ERGA Statement (2014)03 and ERGA Report (2015)11 on the independence of National Regulatory Authorities in the audiovisual sector; http://erga-online.eu/?page_id=14.

[97] CJEU, Case C-424/15, *Ormaetxea and Lorenzo*, 19 October 2016, ECLI:EU:C:2016:780.

framework for electronic communications networks and services ('Framework Directive') (see further below, Q3.4).

Some rapporteurs, like the Dutch, Estonian and Portuguese, consider legal independency requirements for media regulators *at EU level necessary* – especially in light of recent political developments in some Post Soviet and Eastern European countries, the Estonian rapporteurs underline – in order to strengthen the regulators' position, enable them to facilitate the implementation process of EU legislation and therefore catalyse the creation of a single market in this field. This should go hand in hand, we read in the Estonian country report, with closer cooperation between media regulators, notably through the creation of flexible and effective cooperation mechanisms and the creation of a European database of media services. This would allow more effective action against manipulative propaganda, remove possibilities of 'forum shopping' and contribute to the better functioning of the single market.

Other rapporteurs are more sceptical. According to the Czech rapporteur, the absence of independence requirements for the media regulator is not a principal obstacle to the creation of the single market; the primary cause for the fragmentation rather lies in the territorial nature of IP licencing, as well as in cultural and linguistic diversity of the Member States, which creates natural barriers to unification of audiovisual media services. The German rapporteur considers the effect on the internal market of having an independent regulator very hard to quantify, but agrees with most other rapporteurs that the introduction of independence requirements (especially qualitative requirements for the composition and financing of media regulators) at EU level would be a step forward (as long as the form of organization can be decided by the Member States).

Incidents of undue political or commercial pressures on media regulators have been reported in several countries. Government's attempts to undermine the media regulator's independence in Croatia and Greece are described in the respective country reports, as well as in two statements by ERGA of January, resp. April 2016.[98] But also the Italian, French and Maltese rapporteurs are critical of developments in their country in relation to the legal and *de facto* independence of their media regulators. Allegations of political pressure on the Maltese Broadcasting Authority were brought before courts on at least two occasions, but were rejected (demonstrating, however, that it is a very thin line between 'undue

[98] Available from https://ec.europa.eu/digital-single-market/en/news/statement-european-regulators-group-audiovisual-media-services-erga-necessity-independent-media, respectively https://ec.europa.eu/digital-single-market/en/news/erga-statement-alarming-developments-independent-and-effective-functioning-media-regulators. For more details, see e.g.: http://seenpm.org/erga-concerned-media-regulator-croatia/; and https://www.law.kuleuven.be/citip/blog/avms-review-and-media-regulators-independence-the-dancing-procession-of-echternach/ .

pressure' by the Minister and the Minister merely 'alerting' the Chairman of the Broadcasting Authority to check a programme for libellous or defamatory content prior to its broadcast). In Poland, discussions have arisen over the impartiality of the National Broadcasting Council, especially in the 90's in relation to frequency allocation in the emerging TV and radio market, but also more recently, in relation to alleged attempts of censorship under the guise of protecting, amongst others, Christian values or national symbols.

The French rapporteurs describe how the French media authority has gone through successive reforms, resulting in the current constellation of the *Conseil Supérieur Audiovisuel* (which was created in 1989) as an "independent public authority" (since 2013). They consider this process illustrative of the political and commercial pressures that have been exerted on the successive authorities, and their difficult quest for independence. While today, the CSA has a broad regulatory competence (in terms of matters covered), the effect of its regulatory powers is necessarily limited, as a result of the Constitutional Court's decision of 1989 in relation to the CSA's powers. The Constitutional Court interprets Article 21[99] of the French Constitution as conferring on the Prime Minister exclusively the exercise of regulatory powers at national level (except for the powers conferred on the President of the Republic). Although this does not prevent the legislator from entrusting to an authority of the State other than the Prime Minister the task of setting standards for implementing laws, this is however on the condition that this authorization only concerns measures of *limited scope both in terms of their scope and their content*.

The Hungarian report underlines the importance of not only setting legal standards for the regulator's independence, but also ensuring actual independence (sometimes referred to as a 'culture of independence'),[100] *i.e.* the regulator's ability to resist in practice any pressure or attempts of unfair influence from political and market participants in the exercise of powers, and the existence of effective judicial review.

2.5. National Media Policies

Q2.5: What have been the most contentious issues in your country in relation to the application of broadcasting laws? (e.g. rules on commercial communications such as product placement or sponsoring? Unsuitable content for minors on television? The dissemination of hate speech? The role of public service broadcasters? Growing

[99] The French report refers to Article 37 of the Constitution, whereas the decision of the Constitutional Court refers to Article 21.

[100] Cf. 2011 INDIREG study, mentioned above, footnote 69; and W. Schulz, P. Valcke and K. Irion, *The Independence of the Media and Its Regulatory Authorities*, Intellect, 2013.

media concentration?) Do you think that some areas need further harmonisation through the AVMS Directive?

The country reports reflect varying regulatory priorities and issues of discussion. Recurring concerns are however the dissemination of *hate speech and political propaganda* via radio and television (this is mentioned explicitly by the Czech, Croatian, Estonian, Maltese and Portuguese rapporteurs); *protection of minors* (e.g. in Austria, Belgium, Czech Republic, Germany, Portugal and Romania); and enforcement of advertising rules, in particular on *product placement and surreptitious advertising* (as is the case in Austria, Belgium, Germany, Hungary, Ireland, Portugal and Romania; the Maltese rapporteur highlights specific issues in relation to political advertising).

The *financing and independence of public service broadcasters (PSB)* are mentioned by several rapporteurs as contentious issues in their country, e.g. in Greece, Poland, Slovenia and Sweden. The Polish rapporteur notes that existing mechanisms to safeguard objectivity of presented information and political impartiality of PSB are *"woefully inadequate"* and that even *"the concept of "public mission" is so nebulous, superfluous and vague that it is virtually impossible to establish what kind of content falls under it."* The result are fierce discussions and complaints from private media enterprises. This is, however, according to the Polish rapporteur a problem that cannot be solved through EU harmonisation, but that should be sorted out at *national level*. This view is shared by the Croatian rapporteurs, who state that problems regarding the political neutrality of the public service broadcaster should rather be dealt with at national level through effective enforcement of the rules and further strengthening of the independence of the media regulator. Discussions surrounding the funding of PSB are also noted by the Irish rapporteurs. Although complaints from private media actors about breach of EU state aid rules brought the Irish PSB, RTÉ, under scrutiny by the European Commission, the latter found no evidence of illegal state aid and closed its investigation in August 2017.

Impartial news coverage in general (i.e. not limited to PSB) is highlighted as a concern in the Czech and Hungarian country reports.

The Irish rapporteurs also mention *media concentration* as a major concern in Ireland.[101] The media merger regime has been amended in 2014 and now requires an assessment of the public interest in media plurality by the Minister for Communications, on top of the evaluation of the media merger by the competition authority (CCPC) on pure competition grounds. The proposed acquisition in 2017 of CMNL limited, a regional newspaper group, by Independent News and

[101] Media plurality and concentration is also on the media policy agenda in Slovenia.

Media Holdings Limited, publisher of Ireland's best-selling national broadsheet, caused controversy but was withdrawn before the Minister could make a final decision. The BAI, in its report, had recommended that the Minister attach a number of conditions to any approval given to the transaction. In January 2017, an opposition party introduced the Media Ownership Bill in the lower house of the Irish Parliament, but the Bill was defeated in parliamentary proceedings. The rapporteurs, however, expect similar legislative initiatives in the future.

Other country-specific issues that are mentioned in the reports include *must-carry rules* (the Netherlands and Romania); stricter *hourly limits* for advertising applicable to pay-TV operators (this specific Italian situation resulted in a preliminary ruling by the CJEU in 2013 – Case C-234/12, *Sky Italia* – and a ruling by the Italian Constitutional Court in 2015, but is still awaiting a final decision by the Latium Regional Administrative Court); *HbbTV* (Czech Republic); and anticipating on developing technologies and compliance with broadcasting laws in the online domain (the Netherlands).

The country reports do not contain any concrete suggestions for further harmonisation, with the exception of the Greek report, which notes that the AVMS Directive could further proceed to the harmonisation of legal measures guaranteeing *editorial and journalistic independence*. The Estonian rapporteurs consider stronger cooperation among Member States in the area of hate speech and propaganda 'reasonable' considering that the problem affects Europe as a whole. Some rapporteurs note explicitly that further harmonisation in media regulation – for instance with regard to the organisation of the media authority or regulation of public service media – would not be desirable or feasible, due to fundamental differences rooted in the legal cultures of the different countries. According to the Hungarian rapporteur, the EU legislator should rather consider extending the material scope of the AVMS Directive to include new media platforms – as has actually been proposed by the European Commission in its legislative proposal. Also the Dutch rapporteurs stress that harmonisation initiatives in the sphere of media regulation should leave sufficient space to take cultural differences into account (giving the example of the classification of content as harmful or seriously harmful for minors).[102]

[102] With reference to: M. de Cock Buning, "Private Regulation and Enforcement in the EU: Finding the right balance from a Citizen's perspective", in: M. de Cock Buning, L.Senden (ed.), *Private Actors in Regulation* (working title), to be published by Hart Publishers in 2018.

2.6. Targeted or Addressable Advertising

Q2.6: Have there been any initiatives in your country towards the offering of targeted (or addressable) advertising on television or of personalised content? If so, how was this dealt with under broadcasting/data protection laws? Was there any cooperation between the media regulator and the data protection authority? Do you see a need for an EU-wide harmonised approach?

Targeted or addressable advertising on television (allowing different categories of users watching the same linear program to view personalized advertising during the advertising breaks) has recently been introduced in a number of countries, but is often still playing a minor role.

The Czech rapporteur describes how HbbTV targeted advertising is solidifying its presence on the TV screens, moving beyond mere programme or regional targeting towards behavioural targeting (envisaged for Q4 2017). There are no decisions or opinions yet from either the data protection authority or the Council for Radio and Television Broadcasting on the legality of such practices. The rapporteur sees no need for a specific EU-wide harmonised approach in this regard given the early stage of development and limited experience with targeted advertising. In Germany, addressable or personalized TV advertising is being offered through smart TVs with Internet connection (approx. 10 mio. devices) by e.g. the ProSiebenSat.1 TV group, allowing advertisers to differentiate according to regions or weather conditions, but the advertising format is only playing a minor role so far.

In France, the introduction of targeted advertising on television is causing controversy over the protection of personal data and privacy. Regulators' responses (CSA, CNIL) so far have been prudent (*"timides"*, in the words of the rapporteurs), due to a gap between the French law which prohibits the possibility of targeted advertising in traditional broadcasting[103] and the practices of audiovisual media operators, especially new entrants. Regulators' normative initiatives are still limited, do not reflect real – or least official – mutual cooperation,[104] and are complemented by private initiatives (ARPP Recommendation; UFMD Charter). The transparency requirements in the relations between media owners, media agencies and advertisers of the Sapin Law of January 29, 1993 have been extended to the digital media by the so-called Macron law No 2015-990 of August 6, 2015 and have been further implemented by Decree No 2017-159 of February 9, 2017.[105]

[103] Article 13 of Decree No 92-280 of 27 March 1992 (as modified) prescribes that "advertisements must be diffused simultaneously in the whole of the service zone" (with some exceptions).

[104] See eg. CSA, Rapport « Les nouveaux territoires publicitaires : quels enjeux pour la télévision », 4 novembre 2016; http://www.csa.fr/ .

[105] https://www.lexology.com/library/detail.aspx?g=cf58f8eb-37e7-491f-85b4-50a454a6d45d

Also in Italy, the introduction of targeted advertising by Sky, Italy's main pay-TV operator, results in discussions over the legal classification and the applicable rules. The rapporteur considers it undisputable that, despite the difference in technical conveyance (the targeted ads being downloaded and stored in the decoder's hard drive), targeted advertising spots should be considered as being subject to the general rules applicable to advertising on television, both qualitative rules (eg. restrictions concerning certain products like alcohol and medicines) and quantitative rules (i.e. hourly or daily limits). Like in France, a segmentation of viewers on the basis of regions may infringe existing rules which reserve local advertising for local broadcasters and require nation-wide broadcasters to distribute advertising at the same time and with the same content in all the regions concerned.[106] AGCOM, the Italian media regulator has not yet addressed the issue, but the Italian Data Protection Authority issued a decision on 13 July 2016 ruling that targeted advertising is acceptable as long as users are duly informed of the purpose of data processing, the safeguards in place to ensure that data are anonymized and processed only in aggregate form, and the possibility to exercise their statutory rights to information and transparency (pursuant to the Italian Data Protection Code).

The Dutch Data Protection Authority started an investigation in 2016 into the data collection practices of KPN and XS4All, two providers of interactive digital television, and concluded that both operators did not provide adequate information to their customers about how they collected and processed personal data about their TV-viewing behaviour. The Belgian Privacy Commission, through dialogue, reached a 'balanced' agreement with Proximus and Telenet about the conditions under which processing of personal data for the purpose of targeted advertising on television can be carried out in accordance with the Belgian privacy legislation.[107]

Apparently, no country has so far adopted specific rules for targeted advertising on television, nor set up any (formal) cooperation between the media and data protection authorities in this regard. Several rapporteurs, including the Irish, Polish and Swedish rapporteurs, do state explicitly that the general rules on advertising (in statutory law and/or self-regulatory codes) and on electronic commerce and cookies apply in any case.

The German rapporteur notes that *"Europe-wide harmonized rules would be useful, in particular to bring the rules into line with data protection law, which is harmonized in the General Data Protection Regulation 2016/679,"* a view which is shared by the Dutch rapporteur. Also the French, Slovenian and Irish rapporteurs are in favour

[106] Section 38(10) Consolidated Law on Audiovisual and Radio Media Services.

[107] See Belgian coutry report, Q2.6, and the references included.

of European harmonisation in order to consolidate and develop 'good practices' based on public / private co-regulation. By contrast, the Czech rapporteurs see no urgent need for a specific EU-wide harmonised approach.

2.7. Broadcasting and Copyright

Q2.7: Is the specific regime for copyright licensing for TV and radio broadcasting by satellite and cable (pursuant to Directive 93/83/EEC) still relevant in your country? Have similar rules been applied to online transmissions of broadcasting organisations?

Virtually all rapporteurs confirm the continuing relevance of the specific copyright regime for satellite and cable broadcasting (even in Belgium, where the method of 'direct injection' is very common). The Estonian rapporteurs demonstrate this by referring to the recent *Viasat* case, in which the Estonian Court applied the principles set out by the CJEU in *Airfield* (Case C-431/09).[108] Some (like the Finish and Swedish rapporteurs) indicate that the regime has become "less relevant", though, in light of new distribution technologies, in particular online distribution of audiovisual content.

However, none of the countries covered in the reports has apparently extended the country of origin principle and clearance mechanism in the SatCab Directive to online transmissions of broadcasting organisations, as the European Commission has now suggested in its proposal for a regulation laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes (COM(2016)0594).

Whereas new technologies and ways of broadcasting content (incl. new platforms) provide authors and performers with additional means of distributing their works, they were experiencing growing difficulties to negotiate and object against standards provisions in copyright exploitation contracts. This led the Dutch and Belgian legislator to amending their copyright acts in order to give individual authors and performing artists a stronger position in negotiating contracts on copyright transfers with publishers and producers (eg. on 'equitable remuneration', 'bestseller clause', 'non-use clause').

[108] CJEU, Joined cases C-431/09 and C-432/09, *Airfield and Canal Digitaal v. Sabam and Agicoa,* 13 October 2011, ECLI:EU:C:2011:648.

2.8. Cross-Border Portability of Digital Content

Q2.8: What are the main barriers in your country to cross-border portability of digital content? Do you consider that the country of residence of the consumer should be controlled by the service provider on a regular basis? If yes, how to reconcile such requirement with the data minimisation principle under the GDPR?

Several rapporteurs note that the main obstacles to cross-border portability of digital content are not of a regulatory nature, but rather copyright issues, notably the territorial delimitation of licence agreements and the cost-benefit of clearing rights in multiple jurisdictions (Austrian, Czech, German, Swedish, Italian, and Portuguese rapporteurs), the business models of online content service providers (Dutch and French rapporteurs), or language barriers and cultural differences (Portuguese rapporteur).

Estonia has been advocating for ending geo-blocking and proposed the vision of a 5th freedom, free movement of data in the European Union in its 2017 *Vision Paper on the Free Movement of Data*.[109] In other country reports, it is stressed that territorial exclusivity makes it possible to respond to cultural diversity and to a logic of amortization of investments and a reasonable profit in view of the risks taken. This was, for instance, the view of the Polish government in an official position on the European Commission's Communication on "A Digital Single Market Strategy for Europe", *i.e.* that the territoriality principle allows for customisation of content to reflect country specificity and particular customers' needs. The French rapporteurs refer to economic studies, a.o. commissioned by the European Commission, in which the beneficial / pro-competitive effects related to territorial exclusivity are widely documented. They note that the demand for cross-border offers concerns only a very small proportion of content which is apt for exploitation on a pan-European scale. The players in the sector should therefore remain free to adapt their contractual practices to a demand that has a strong local dimension, linked to the tastes of consumers and the control or lack of language.

This demonstrates the need to strike a balance between reasonable demands of consumers regarding portability, on the one hand, and the economic interests of the audiovisual sector, on the other hand. Most rapporteurs mention explicitly that this issue should be tackled EU-wide and therefore welcome the newly-adopted Regulation on cross-border portability of online content services (2017/1128/EU), including the limits it imposes on the verification by service providers of the subscriber's Member State of residence in order to ensure

[109] Estonian Vision Paper on the Free Movement of Data – the Fifth Freedom of the European Union, https://www.eu2017.ee/sites/default/files/inline-files/EU2017_FMD_visionpaper.pdf

compliance with EU privacy and data protection law.[110] According to Article 5 of the new Portability Regulation, the provider should only check the subscriber's Member State of residence at the conclusion and upon the renewal of a contract and in reasonable doubt, which is considered to represent an appropriate compromise between the interests of the providers and the users (see, in particular, the German country report).

3. Digital Infrastructures

Telecommunications networks and services are the backbone of our information society. In recent decades, the EU has adopted a harmonised regulatory framework for electronic communications to improve competition, drive innovation, and boost consumer rights within the European single market (the electronic communications regulatory package of 2002, as amended in 2009).[111] In 2015, it adopted rules on *net neutrality (open internet)* which it labelled as a *"major achievement for the Digital Single Market."*[112] The rules in Regulation (EU) 2015/2120 prescribe that, in principle, all traffic has to be treated equally, and that every European must be able to have access to the open internet and that all content and service providers must be able to provide their services via a high-quality open internet. Under these rules, blocking, throttling and discrimination of internet traffic by Internet Service Providers (ISPs) is not allowed in the EU, save for three exhaustive exceptions (compliance with legal obligations; integrity of the network; congestion management in exceptional and temporary situations) and users are free to use their favourite apps and services no matter the offer they subscribe to.

The EU also launched several initiatives to promote investment in broadband networks supporting high-speed Internet. In September 2016, in the light of its Digital Single Market strategy, the Commission adopted a set of measures – the so-called "connectivity package"[113] – to place the EU at the forefront of internet connectivity and achieve a European 'Gigabit Society', including a proposal for a new European Electronic Communications Code.[114] The Code further stimulates competition, and strengthens the internal market as well as consumer rights and wants more forward-looking and simplified rules that make it more attractive for all companies to invest in new top-quality infrastructures in the EU.[115]

[110] For more information, see the Institutional Report. The Italian and Swedish reports also contain an insightful discussion of Regulation 2017/1128/EU.

[111] For more information, see: https://ec.europa.eu/digital-single-market/en/telecoms-rules

[112] See: https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality

[113] https://ec.europa.eu/digital-single-market/en/connectivity-european-gigabit-society

[114] https://ec.europa.eu/digital-single-market/news-redirect/34112

[115] For more information, see the Institutional Report and https://ec.europa.eu/digital-single-market/en/news/review-electronic-communications-regulatory-framework-executive-summaries.

3.1. Net Neutrality/Open Internet

Q3.1: Did your country have rules on net neutrality in place before the adoption of Regulation (EU) 2015/2120? If so, were they more or less strict in comparison to the Regulation? What is the national approach towards practices of zero-rating (which are not explicitly prohibited by the Regulation)?

Most countries followed the European Commission's initial wait-and-see approach with regard to net neutrality and did not adopt any specific rules (in addition to transposing the consumer-oriented transparency requirements adopted in the 2009 Citizens' Rights Directive[116]). Pending national measures (e.g. in Luxembourg, Belgium and Portugal) were stopped after the European Commission adopted its Telecoms Single Market proposal in September 2013 that finally resulted in Regulation (EU) 2015/2120. In Germany, for instance, the provision introduced in 2012 into the Telecommunications Act (§41a) to delegate powers to government to adopt a decree on net neutrality was never implemented and was abolished again in 2017. The Italian draft bill on net neutrality that was introduced in 2014 (known as the "DLL Quintarelli") is still being discussed in Parliament, but is criticized by industry for creating the risk of unnecessary overlap and potential inconsistencies with Regulation (EU) 2015/2120.

In a number of countries, the telecommunications regulator adopted (non-binding) position papers or guidelines on net neutrality. The Austrian NRA, for instance, published a position paper in May 2013 with seven principles on net neutrality, whereas the Czech Telecommunications Office (CTU) adopted in January 2014 its *"General rules and recommendations for use of data traffic management in providing an Internet access service"*, which contained rules very similar to the ones in Regulation (EU) 2015/2120. Also in Norway, national guidelines have been drawn up by the Norwegian Communications Authority (NKom) in collaboration with industry stakeholders, setting out principles for the handling of data traffic by internet service providers. Although these guidelines did not have formal legal status, they worked effectively, according to the rapporteurs. They have been replaced by legally binding provisions in March 2017 to transpose Regulation (EU) 2015/2120 into Norwegian law.

Only in *the Netherlands, Finland* and *Slovenia*, legally binding measures were in place prior to the adoption of Regulation (EU) 2015/2120. In Finland, specific

[116] Directive 2009/136/EC of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, *OJ* L 337, 18 December 2009, p.11.

rules on net neutrality were introduced on 1 January 2015 in the Information Society Code. They have already been replaced in 2016 by a direct reference to Regulation (EU) 2015/2120 (in Section 110 of the Code). The Code did (and does) not take any position on zero-rating (see below), but gives a relatively wide discretion to the Finnish Communications Regulatory Authority to implement and give more specific orders on technical characteristics of internet access or on commercial practices of operators. In the Netherlands, rules on net neutrality have been applicable since 1 January 2013, when the Act of 10 May 2012 amending the Telecommunications Act entered into force. The Dutch rapporteurs explain that these measures still exist and can be considered more stringent compared to the rules in the Regulation. This is notably the case with regard to zero-rating which is explicitly prohibited by Article 7.4a of the Dutch Telecommunications Act. After the Netherlands Authority for Consumers and Markets (ACM) took action against *T-Mobile* for its 'data free music' service on the basis of this provision, the Rotterdam District Court found on 20 April 2017 that such categorical prohibition is not compatible with Regulation (EU) 2015/2120, but that a case-by-case assessment is needed, as suggested in BEREC's Guidelines on Net Neutrality of August 2016.[117] ACM decided not to appeal the judgment. The Slovenian Electronic Communications Act introduced net neutrality rules in 2012, but was amended in 2017 to ensure consistency with Regulation (EU) 2015/2120.

Regulation (EU) 2015/2120 does not explicitly prohibit zero-rating[118] and allows business models based on different volumes of data, speeds and quality characteristics under certain conditions. Most country rapporteurs state that their telecommunications regulators pro-actively monitor operators' practices, in accordance with the Regulation and BEREC's 2016 Guidelines. In some instances, this has effectively led to sanctions. The Hungarian NRA, NMHH, was among the first to enforce the Regulation. The NMHH investigated in December 2016 whether Magyar Telekom's 'Unlimited TV & Film' option (giving unlimited access to the *TV GO* and *HBO GO* services for 24 hours without deducting any data traffic from the subscriber's package or reducing data speeds, which

[117] BEREC Guidelines on Net Neutrality, August 2016, http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules.

[118] The BEREC Guidelines describe zero-rating as a commercial practice where an ISP applies a price of zero to the data traffic associated with a particular application or category of applications (and the data does not count towards any data cap in place on the internet access service). Zero-rated services often include social media, music or video streaming highlights of sport events. While zero-rating may offer some benefits for consumers, the concern from a competition point of view, as the Irish rapporteurs explain, is that *"the practice of zero-rating may enable network operators to pick winners by tilting the playing field in favour of particular Over-The-Top ('OTT') service providers. A zero-rated OTT service provider would have an advantage over rivals whose end-users would have to pay data charges to use."*

normally apply after a certain amount of traffic is used) complied with the net neutrality rules. As a result, NMHH ordered Magyar Telekom to suspend any offer of zero-rated over-the-top (OTT) video services to its mobile subscribers. In January 2017, NMHH ordered *Telenor Hungary* to suspend as well its zero-rated offer since it discriminated amongst certain types of contents (such as chat and social media services). NMHH found that such commercial practice might encourage end-users to use the zero-rated services to the detriment of other competing online services, possibly distorting competition.

Also in Germany, Italy, Slovenia and Sweden, cases are reported in which the NRA took action against zero-rating practices. Already in 2015, under its national law, the Slovenian Agency AKOS carried out five inspection procedures against mobile operators as internet access providers (including Telekom Slovenije and Si.mobil, the two largest operators in Slovenia). The operators offered several services of their own (like free music streaming, free cloud storage service, free TV on mobile devices and free access to certain apps) to end users without charging for data transfer. In all cases, AKOS considered such practice of giving priority to their own zero-rated services to be a form of price discrimination, in violation of the national net neutrality rules. The decisions were, however, overruled in July 2016 by the Administrative Court. A critical assessment in 2016/2017 by the German *Bundesnetzagentur* of two offers by *Deutsche Telekom* resulted in Deutsche Telekom discontinuing one of the offers for new customers; the other offer ('Stream On'; on the market since April 2017) is still under investigation. AGCOM in Italy adopted a cease and desist order against one telecommunications provider because of unfair practices of discriminating internet traffic. The Swedish NRA *(Post- och telestyrelsen)* adopted two decisions resulting in the prohibition of *Telia's* zero-rating practices (which entailed that selected applications could still be accessed when the data cap was reached) and the imposition of conditions on such practices by *Hi3G* (which agreed to discontinue selected zero-rated music applications once the data cap is reached). Both cases are described in the country report. The appeal in the *Telia* case before the Administrative Court of Appeal is still pending and may lead to a reference for a preliminary ruling to the CJEU, according to the rapporteur. By contrast, none of the three zero-rating cases that the Norwegian NKom looked into resulted so far in any sanctions, despite the fact that NKom is still rather sceptic towards zero-rating (the Norwegian rapporteurs note that NKom's previous guidelines on net neutrality were stricter in relation to zero-rating, like the Dutch Telecommunications Act). Also the Belgian Institute for Postal Services and Telecommunications (BIPT) has monitored zero-rating practices implemented by *Proximus* and other operators, but saw no reason to take action.[119]

[119] See http://www.bipt.be/en/operators/telecommunication/protection-of-consumers/bipt-analysis-of-zero-rating-of-apps-in-the-proximus-offers. BIPT did, however, request *Lycamobile* to remove from its

Also in other countries, emerging zero-rating practices result in concerns expressed by the telecommunications regulator. The Irish rapporteurs, for instance, refer to ComReg's Draft Electronic Communication Services Strategy 2017 – 2019, whereas the Austrian rapporteur mentions that its telecommunications regulator, RTR, considers the absence of a categorical ban on zero-rating in the Regulation as a risk for long-term net neutrality and the innovative power of the internet. Only in a few countries (like Estonia, Spain, Croatia and Poland), rapporteurs note that zero-rating practices are not applied in practice by operators, or are not an issue of concern.

3.2. Telecommunications Single Market

Q3.2: Should the EU go further in creating a single market for telecommunications networks or services (and introduce e.g. an EU-wide licensing scheme)? Did your national authorities adopt any special broadband measures and were they the result of EU intervention or adopted at own initiative?

As the Hungarian rapporteurs note, the idea of an *EU-wide licensing scheme* was suggested by the European Commission in its Telecoms Single Market (TSM) proposal in 2013, with special emphasis on the unification of spectrum assignment and on licensing (upon simple declaration) of electronic communications service providers. The discussions in the European Parliament and the Council demonstrated the political sensitivity surrounding these issues, resulting in a much more modest Regulation (EU) 2015/2120 finally being adopted (only covering roaming and net neutrality). Views from the rapporteurs are *divided* when it comes to a pan-European licensing system: whereas the German rapporteurs consider the idea 'superfluous', the Hungarian, Portuguese and Romanian rapporteurs note that the implementation of a one-stop-shop system and the development of a common, harmonised and simplified notification format might reduce administrative burdens and facilitate the cross border provision of services (although the Portuguese rapporteurs stress the necessity to adequately determine the extent of such licences and the Romanian rapporteurs find that providers should maintain the freedom to choose between notification at EU or

general terms and conditions the prohibition to share the Internet connection (tethering), considering this an unjustified restriction of the consumer's choice of terminal equipment (cf. recital 5 of Regulation (EU) 2015/2120 and BEREC Guidelines 2016, para. 27). Tethering was also considered a violation of net neutrality rules by the Electronic Communications Council of Slovenia, but the Agency in charge (AKOS) was of the opinion that the limitation of the use of internet connection at the level of a device was not covered by the national Electronic Communications Act (contrary to Regulation (EU) 2015/2120 which was not yet in force at that time).

at national level). The Belgian rapporteurs, despite being in favour of further steps towards the creation of a single market for electronic communications, are sceptical with regard to an EU-wide licensing scheme, as it directly affects the national sovereignty of the Member State. They also note that the current trend is more towards fragmentation of the internal market, citing the divergence in legal qualification of Skype Out as an example (with some countries considering the service merely an information society service, and other countries – including Belgium – considering it to be an electronic communications service).[120]

Also the Finnish, Italian and Greek rapporteurs express themselves in favour of further strengthening the single market for telecommunications networks and services. According to the Spanish rapporteur, networks in Member States are increasingly divergent (in terms of fibre deployment, architectures, technical solutions, etc.) and (too) little action has been taken at EU level to harmonise the markets, creating obstacles to provide EU-wide services, particularly in the business segment. By contrast, the Maltese rapporteur cites the view of the Malta Communications Authority, which is quite critical of the European Commission's pending proposals in the draft European Electronic Communications Code (EECC) regarding EU-wide licensing schemes: *"While at face value, these [proposals] seem to be decreasing bureaucracy, in reality these would be shifting local enforcement powers up to the Commission. The Commission's Impact Assessment did not prove that there exist market failures or that the current rules create any barriers to entry or that implementation should be at an EU level. Therefore, while a single market for telecommunications networks and services is very important, having for example EU-wide licensing schemes do [sic] not necessarily benefit the single market but might as well run counter to this same objective".*

When it comes to the further harmonization of *spectrum management*, no rapporteur expresses a favourable view. As the Portuguese rapporteurs rightly note, discussions about the EECC demonstrate that Member States and NRAs are reluctant to give up control on the definition of conditions associated with spectrum assignment. The Hungarian rapporteurs argue that it might be reasonable to let Member States have sole competence over spectrum assignment, due to the politically sensitivity (since the income from spectrum assignments "belongs" to the national budget) and technical specificities (with needs varying from Member State to Member State for different bands of spectrum according to various characteristics such as use of Internet, demand of the service providers, etc.).

[120] On 30 May 2016, the BIPT imposed a 223,454 EUR administrative fine on Skype for refusing to notify itself as a provider of electronic communications services for its SkypeOut service and, hence, by-passing the obligations imposed by the legislation applicable to operators. See http://www.bipt.be/en/operators/press-release/123-skype-fined-by-bipt-regarding-the-skypeout-telecom-service. Appeal before the Brussels Court of Appeal is pending.

Basically all countries covered in the reports have adopted special measures to stimulate the deployment and uptake of *broadband networks*, usually in accordance with the EU's broadband targets for 2020 set in the context of the Digital Agenda for Europe (DAE) and the Digital Single Market (DSM) strategy (i.e. NGN coverage allowing internet connectivity of 30 Mbps or more for all citizens and NGN use of 100 Mbps or more by 50% of households by 2020).[121] Romania adopted its National NGN Infrastructure Development Plan; Estonia its EstWin project; Hungary its Digital Welfare program of which the "Super Fast Internet Program" is a sub-program; Poland its "Digital Poland 2014-2020" programme; Slovenia its "Development strategy for the information society until 2020"; etc. Several rapporteurs mention subsidies and state aid plans underpinning the roll-out of next-generation broadband network, which usually required the approval of the European Commission under EU state aid rules (as is mentioned, for instance, in the Estonian country report). In Estonia and Poland, EU structural funds are being used to (co-)finance broadband projects, whereas Ireland relies on the European Regional Development Fund to finance the deployment of FTTH in the so-called "Intervention Area" (i.e. the area where commercial providers acting alone will not invest in high-speed networks).

Some countries, like Austria, Hungary or Sweden, have set more ambitious goals than the EU targets. The Hungarian "Super Fast Internet Program" aims to achieve that all households have access to 30Mbit/s Internet by the end of 2018, i.e. two years prior to the deadline fixed by the European Commission. The Swedish Broadband Strategy adopted in December 2016 envisages 100 Mbps by 2020 for 95% of households and businesses and 1 Gbps for 98% by 2025. The Swedish rapporteur also refers explicitly to Sweden's transposition of Directive 2014/61/EU and the fact that it agreed to draw up a common development plan for 5G with the Nordic and Baltic countries. 5G strategies are also mentioned by the Hungarian and Italian rapporteurs. In Hungary, almost fifty government institutions, companies, business chambers, universities, research institutes and professional and civic organisations have established – as a national initiative – in June 2017 the so-called "5G coalition" with the aim to support the development of the next generation of mobile telecommunications technology in Hungary. The coalition's goals include drawing up a 5G development strategy, establishing a testing environment that gives Hungary a say in setting global 5G standards and becoming the first to adopt those standards from 2020. In Italy, a 5G trial was launched in five cities (Milan, Prato, L'Aquila, Bari and Matera).

[121] For more details, see: https://ec.europa.eu/digital-single-market/en/broadband-strategy-policy . In September 2016, the European Commission adopted three new main strategic objectives for the availability and take-up of very high capacity networks (100 Mbps-1 Gbps and 5G) by 2025 in its strategy on Connectivity for a European Gigabit Society.

Spain presents a quite exceptional situation, with three competing fibre networks and one of the highest penetration rates of FTTH in the EU. Ironically, this is the result of inactivity of the Spanish NRA, CNMC, who excluded access to fibre from the *ex ante* regulatory obligations imposed on Telefonica in 2009, but then waited until 2016 to carry out another market analysis (actually resulting in a seven year "regulatory holiday" for Telefonica). By that time, competition from alternative operators like Orange and Vodafone – who had no alternative than to deploy their own fibre network – had already emerged and CNMC decided to exclude access to fibre in all major cities from regulatory obligations. Also Malta paints a peculiar picture with 100% coverage of fixed broadband at speeds of at least 30 Mbps up to 250 Mbps. Investment was fully privately funded and mainly driven by competition. MCA adopted a number of initiatives to stimulate demand and increase the take-up of broadband services, but none was the result of EU intervention.

3.3. Spectrum Management

Q4.3. Are there legal issues on spectrum management in your country? If yes, how have they been solved?

Several country reports mention legal challenges that were brought against governmental or NRA decisions about spectrum allocation and assignment.[122] Both the Dutch and Swedish rapporteurs mention that in a few cases, decisions or decrees have been appealed before courts, but courts have generally ruled that those were not in breach of EU legislation and upheld the contested measures. This was also the case in the Czech Republic, where Vodafone initiated a legal dispute about new frequencies that became available in the GSM spectrum range. According to Vodafone, it was entitled to these frequencies, even though it was not a holder of a licence needed for assignment in this frequency range, because it was the first to apply and because of 'historical inequality'. The Czech courts confirmed the decision of the Czech Telecommunication Office and dismissed

[122] Spectrum allocation determines what blocks of frequencies are used for what specific purpose under a set of technical and operational rules (for example, the allocation of the 700 MHz band for mobile services that eventually became 4G/LTE mobile broadband). Spectrum assignment determines who gets to access blocks of the spectrum over a specific geographic region in support of a specific service, usually in the form of a license or an assignment. A typical example of this would be a major cellular service provider (e.g., T-Mobile or Vodafone) licensed to operate specific blocks of spectrum in the 700 MHz band, or the military being assigned a band for its exclusive use. Source: National Academies of Sciences, Engineering, and Medicine. 2015. *A Strategy for Active Remote Sensing Amid Increased Demand for Radio Spectrum*. Washington, DC: The National Academies Press.

Vodafone's claim, stating that frequencies should be obtained on the basis of a transparent selection procedure and not on the basis of 'historical inequality'. The Greek rapporteur refers to legal issues that have arisen from the lawfulness of imposing restrictions to the spectrum user's rights to be granted.

As DTT (Digital Terrestrial Television) is traditionally very popular in Spain, spectrum policies to favour mobile services over DTT services have created conflicts in recent years. The Spanish rapporteurs note, however, that spectrum redistribution might become less of an issue in the future with the growing penetration of fibre deployment. A similar conflict may arise in Italy, with the envisaged transition of the 700 MHz band – currently predominantly occupied by TV channels (holding 20 year-term licenses granted in 2012) – to 5G, which should be completed by 2020 pursuant to EU law.[123]

Interestingly, the Hungarian rapporteurs refer to the dilemma that may arise between efficient use of spectrum and effective competition. Such dilemma was created in 2015 when the Hungarian regulator NMHH approved the agreement between Magyar Telekom and Telenor on spectrum sharing and lease of the 800 MHz band. Secondary frequency trading is a means to guarantee free competition in the telecommunications market (and is therefore supported in principle by the EU). However, the two operators involved now dispose over a much bigger amount of spectrum than the third operator, Vodafone Hungary.

In Belgium, the proliferation of taxes imposed on mobile operators by local and provincial authorities continues to cause problems, as the Court of Justice left margin for manoeuvre in *Ville de Mons v. Base Company* by ruling that the Authorisation Directive is only applicable to taxes when the trigger for that tax is linked to the general authorisation procedure, but does not preclude other taxes on pylons, masts or antennas.[124] Mobile communication operators are also faced with regional divergences and legal uncertainty in the area of regulatory standards for non-ionizing radiation. Whereas Council Recommendation 1999/519/EC of 12 July 1999 recommends a maximum power density, this ceiling is not mandatory. Regional authorities have substantially lowered this threshold, some more than others for reasons probably not devoid of electoral considerations. The Belgian rapporteurs point out that such lack of future predictability may be detrimental to the modernization of networks and the deployment of 5G.

[123] EC Implementing Decision 2016/687 of 28 April 2016 on the harmonisation of the 694-790 MHz (700 MHz) frequency band for wireless broadband; http://europa.eu/rapid/press-release_IP-16-207_en.htm.
[124] CJEU, Case C-346/13, *Ville de Mons v. Base Company*, 6 October 2015, ECLI:EU:C:2015:649; see: http://equal-partners.eu/en/news/taxes-on-gsm-pylons-and-masts.

3.4. Telecoms Regulator's Independence

Q4.4. Have questions linked with the independence of NRAs been raised in your country? If yes, did they lead to legal challenges? How have they been solved?

In the last decade, the European Commission has started several infringement cases concerning the independence of NRAs or effective structural separation (between regulatory functions and ownership/operational functions), amongst others against Belgium, Bulgaria, Estonia, Latvia, Lithuania, Luxembourg, Poland, Romania, Slovakia, and Slovenia.[125] In a limited number of instances, this has resulted in a referral to the CJEU (not all of which led to an actual judgment). The CJEU has also interpreted the independence requirements in the EU Framework Directive in a number of preliminary rulings, some of which are referred to in the country reports (see the example of Spain below).

The majority of rapporteurs make no mention of specific disputes in recent years[126] and stress that the independence and autonomy of the telecommunications regulator is guaranteed by law (see, for instance, the Austrian, Czech, German and Irish country reports). Although no legal challenges have been brought before courts, the Maltese and Dutch rapporteurs refer to legal doctrine in their country in which (fierce) criticism was voiced on the possibility for the Minister to give directions to the regulator (as created by Article 6 of the Malta Communications Authority Act),[127] respectively the absence of possession of its own legal personality, personnel or budget (as is the case with the Dutch ACM). Also the Italian rapporteur notes that tension arises from the fact that members of AGCOM are elected by Parliament, which creates an inherent connection between political parties and the members of the NRA. Nonetheless, the law mitigates this risk by requiring candidates to possess specific expertise and independence. In Sweden, allegations have recently been made in the media by a private mobile operator, accusing the Swedish NRA of favouring the partly State-owned operator Telia in the context of the spectrum auction for the 700 MHz band. Those accusations were however not substantiated and have been

[125] For an overview, see: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Infringement%20procedures%20opened%20for%20incorrect%20implementation.pdf

[126] In Norway, discussions over the independence of NKom date back from the late 1990s, when the Ministry of Transport and Communications was at the same time the owner of *Telenor* and the appeals body for decisions taken by NKom. After the EFTA Surveillance Authority issued a reasoned opinion to Norway, the ownership of Telenor was transferred to the Minister of Trade and Industry to ensure structural separation between ownership and regulatory functions (as required by the EU telecommunications framework in force at that time). NKom is now an autonomous agency of the Ministry of Transport and Communications, and is self-financed, primarily through fees and charges.

[127] Except on matters related to *ex ante* market regulation and dispute resolution.

rejected by the NRA. Belgium adapted its law in 2015 after the European Commission had decided to refer it to the Court in October 2014 because decisions of the regulator could be suspended by the government, and its multi-annual strategy had to be approved by the Government as well.[128]

The Greek and Polish rapporteurs note that discussions have mainly arisen in relation to the independence of their media regulator, rather than of their telecommunications authority, or in relation to the blurred division of competencies between the two.

Several countries have in recent years *restructured* their regulatory authorities, often merging previously distinct sector regulators from the telecommunications, postal, rail and energy industries with each other (think of *Bundesnetzagentur* in Germany, *HAKOM* in Croatia) and/or with the competition and consumer protection agencies (like *ACM* in the Netherlands and *CNMC* in Spain) for efficiency reasons. In some instances, this led to disputes about the regulator's independence, as was the case in Romania, where the Government restructured *ANCOM* four times in five years by way of emergency legislation and removed its president despite an opposite ruling by the Bucharest Court of Appeal. The European Commission sent letters of formal notice twice but eventually closed the case after the Romanian Parliament adopted a new legal framework strengthening the independence of the telecoms regulator.[129] In Croatia, the number of members of the Council of *HAKOM*, the Croatian Regulatory Authority for Network Industries, was lowered from seven to five in 2012, putting its independence into question.

But it were the discussions that emerged over the Spanish Law 3/2013 which led to the creation of the National Markets and Competition Commission *(CNMC – Comisión Nacional de los Mercados y la Competencia),* which gave the CJEU an opportunity to clarify the scope of Member States' institutional autonomy in light of independence requirements in the Framework Directive. Law 3/2013 centralised tasks relating to market regulation in sectors previously supervised by different regulatory authorities with the intention "to increase economies of scale and ensure consistency and effectiveness in the regulation of all network industries for the benefit of consumers and users". In practice, the National Competition Authority and the National Regulatory Authorities with sector specific competences in telecommunications, audio-visual media, postal services, energy,

[128] http://europa.eu/rapid/press-release_IP-14-1145_en.htm. The Commission suspended its referral and eventually closed the infringement case following the adoption and notification by Belgium of a law amending the rules for the regulator's functioning; https://ec.europa.eu/digital-single-market/en/news/commission-closes-belgian-telecom-regulators-independence-case.

[129] See the European Commission's press releases of 29 January 2009 (IP/09/165), 5 May 2010 (IP/10/519), and 24 November 2010 (IP/10/1557).

railways and airports were merged into one single cross-sectorial NRA, CNMC. The President of the former Telecommunications Market Commission *(CMT – Comisión del Mercado de las Telecomunicaciones),* as well as one of the members of the board, challenged their dismissal which was the result of the reform process, arguing that it constituted a breach of the independence requirements in Directive 2002/21/EC (Framework Directive). In a preliminary ruling of 2016, the CJEU found that *"Directive 2002/21/EC [...] is to be interpreted as not precluding, in principle, national legislation which entails the merger of a national regulatory authority [...] with other national regulatory authorities".* However, the CJEU also ruled that Article 3(3a) of the Framework Directive *"is to be interpreted as precluding — on the sole ground that an institutional reform has taken place involving the merger of a national regulatory [...] the dismissal of the President and a board member, members of the collegiate body running the merged national regulatory authority, before the expiry of their terms of office, in the absence of any rules guaranteeing that such dismissals do not jeopardise the independence and impartiality of such members."* (Case C-424/15, *Ormaetxea and Lorenzo*; see above Q2.4). The conflict was finally solved by (re)appointing both the former President and member of the board of CMT as members of the board of CNMC in the regular renewal process of board members in 2017.

But the fact that so many powers have been concentrated in a single authority, CNMC, has also been criticised at the national level. The rapporteurs note that competences traditionally granted to the sector specific authority have been given to the Ministries (e.g. in the case of licenses, notifications and numbering, control of net neutrality rules). The rationale was to reduce the concentration of powers in a single independent authority, but it is doubtful whether this is in accordance with the relevant EU directives (particularly in the energy sector). The internal functioning of a complex institution like CNMC has raised doubts. Although the concentration of competition law and sector specific regulation in the same institution was supposed to avoid contradictions in the application of both sets of rules to the same cases, conflicts are still possible, since two chambers were created to decide on competition law issues, on the one hand, and regulatory issues, on the other hand. Intense exchange of reports among the services of the competition directorate and the relevant sector specific directorate, as well as joint meetings of the competition and regulatory chambers to decide upon the most relevant cases, should overcome this problem. Scepticism has been voiced about the ability of the five members of the regulatory chamber to actively supervise the intervention in industries as complex as telecommunications, energy, transport, and posts. The rapporteurs note that a political agreement has been reached to reform CNMC and to split it (again) in two different authorities, one for competition law and another for sector specific regulation.

4. Data in the digital economy

During the XXVIII FIDE Congress, on Friday 25 May 2018, the General Data Protection Regulation (GDPR) will start to apply. It is labelled *"the most important change in data privacy regulation in 20 years"* on the Commission's GDPR portal (https://www.eugdpr.org/). It took four years of preparation and debate before the GDPR was finally approved by the EU Parliament on 14 April 2016. It replaces the Data Protection Directive 95/46/EC and is designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

The GDPR will be 'particularised' by the ePrivacy Regulation,[130] which will replace the ePrivacy Directive but is still under discussion with the Council and the Parliament. Whereas the GDPR regulates data processing activities in a sector-neutral way, the ePrivacy Regulation deals with specific issues in the telecommunications sector in order to ensure the confidentiality of communications. The intention is to broaden the scope to new OTT communications players like WhatsApp, Facebook Messenger and Skype, and also covers IoT/M2M communications.

Besides these initiatives to protect the EU citizens' fundamental rights to privacy and the protection of their personal data in an increasingly digitised would, the European legislator has recently also taken an interest in defining the legal framework for *non-personal* data, in order to ensure the free flow of data throughout the EU and to clarify rights of ownership, access and use.[131] In September 2017, the Commission published a Proposal for a Regulation on a framework for the free flow of non-personal data in the European Union.[132] This initiative aims to fully reap the opportunities offered by new digital technologies, such as cloud computing, big data, artificial intelligence and the Internet of Things and unlock the potential to exploit the value of the EU data market.

4.1. GDPR

Q4.1: How is your country preparing for the entry into force of the General Data Protection Regulation in May 2018? Are there any specific legislative proposals or executive measures in preparation?

In virtually all countries discussed in the reports, intense preparations for the application of the GDPR take place at various levels, involving public authorities

[130] See https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation
[131] See https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data
[132] COM(2017) 495. See the Institutional Report for further details.

as well as the private sector. This section will focus on legislative and regulatory initiatives, whereas the next section (Q4.2) will cover actions taken by the private sector. Please note that most country reports were finalised in the summer of 2017; consequently, the following summary does not take into account the latest developments that took place in the second half of 2017.

As the Dutch rapporteurs note, the important changes in the European legislative framework for data protection require an overhaul of existing national data protection rules. Although the GDPR is directly applicable in Member States, it contains numerous referrals to national legislations as well as various exemptions requiring recourse to domestic rules, and some articles allow for discretion at Member State level. The GDPR also triggers a myriad of amendments to laws and regulations in other fields, e.g. financial law, immigration, taxation and customs, elections, education and research etc. (according to the Polish rapporteur, it is estimated that approximately 600 acts currently in force require reviewing to make them GDPR-compatible).

Member States are preparing, or have already adopted, various bills to amend or repeal existing national data protection acts. The new bills are being, or have been, discussed in inter-ministerial or multi-stakeholder working groups, and are based in some countries, like France, on extensive studies, reflection documents and public consultations. The proposed texts revise existing national rules to ensure their consistency (and avoid duplication) with the GDPR, and also give effect to, and provide for derogations from, the GDPR. They specify aspects left by the GDPR to the discretion of the Member States, e.g. the journalist and media exemption, public access to official documents, data protection in the context of employment, the age limit of a child's consent, etc. The majority of them simultaneously transpose the 'Police Directive' (Directive 2016/680).[133] Sometimes the proposals entail the extension of the application of certain provisions of the GDPR to activities which fall outside its scope (like in the case of Sweden, where it is suggested to extend the rules to the processing of personal data covered by the EU Common Foreign and Security Policy).

As the GDPR also profoundly changes the regulatory and enforcement landscape (triggering, for instance, a significant increase of European cooperation and *ex officio* investigations), the national bills usually also entail an institutional reform, setting out the rules for the organisation and functioning of the (new or reformed) independent national Data Protection Authority (hereafter: DPA). In

[133] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ* L 119, 4 May 2016, p.89–131.

Ireland, for instance, the "General Scheme of Data Protection Bill 2017" envisages that the current Data Protection Commissioner will be replaced by a new legal entity to be named the Data Protection Commission, with the potential for up to three individual Commissioners to be appointed (in order to be able to deal with the expected additional workload under the GDPR and the "one stop shop" mechanism in particular). The Irish Bill also grants broad ministerial powers to adopt restrictions on the exercise of data subject rights in as far as necessary *"to safeguard important objectives of general public interest"* (of which the Bill provides a non-exhaustive list). Belgium adopted its *Law Establishing the Data Protection Authority,* which entails a complete overhaul of the existing Belgian Privacy Commission into a reinforced Data Protection Authority, on 3 December 2017.[134]

Some of those 'implementing' bills, like the German *Data Protection Adaptation and Transformation Act,* have already been promulgated. With the adoption of the *Law for a Digital Republic of October 7, 2016*, France even anticipated the application of the GDPR by including in its national law a first reference to the digital 'right to be forgotten' (see below, Q4.4), a right to data portability and a reinforcement of the powers of the French DPA, CNIL. It is now in the process of preparing a new legislative proposal to adapt the French Data Protection Act of 1978 to the GDPR (Act No 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties). But several proposals are still under discussion in government working groups or national parliaments, and some rapporteurs, like the ones from Austria, Czech Republic, Croatia and Hungary, doubt whether the bills in their country will effectively be promulgated by the time the GDPR starts to apply (May 25, 2018).[135]

Whereas in several Member States (e.g. in Finland or the Netherlands), governments opt for *maximum harmonisation* of their national rules with the GDPR (*i.e.* using the margin of manoeuvre left for Member States scarcely or in a 'policy-neutral' manner), other Member States use their *margin of discretion* to reflect national policy choices. A good illustration of this is Sweden, which has a very strong tradition in protecting freedom of speech and of information. This tradition is reflected in the proposed general exemption from the GDPR for the processing of personal data which falls within the scope of the Fundamental Law on Freedom of Expression and the Freedom of the Press Act, which is complemented by exemptions for the processing of personal data for journalistic purposes or for academic, artistic or literary expressions, and for the processing of personal data

[134] Another Belgian law on the implementation of the GDPR (establishing specific rules for certain sectors, like the judiciary and the public sector, and defining the exceptions for journalistic, artistic, scientific and statistical purposes) is in preparation.

[135] In some cases, the delay is caused by sensitive discussions over constitutional aspects, such as the division of powers between the federal and regional authorities in Austria.

which falls within the scope of the Swedish principle of public access to official documents. The Swedish rapporteur notes that this special treatment of mass media companies and of any Swedish person who has obtained a so-called 'publishing certificate' is causing tensions, since such actors are exempted from any obligation under Swedish data protection law and the Swedish DPA is in principle not entitled to monitor them. Discussions particularly relate to the publication of sensitive data (e.g. health data, political opinions or criminal convictions) published on websites or included in search engines. According to the rapporteur, a recent complaint from Mr. Max Schrems against the Swedish mobile application "Truecaller" (which holds a publishing certificate even though its business is not primarily concerned with free speech) illustrates the risk of Sweden being used as a safe haven by certain companies in order to circumvent more restrictive data protection rules in other Member States.

Sometimes political views that national governments unsuccessfully tried to introduce in the GDPR, resurface in the national implementation texts. The attempt of the German minister to allow more flexibility in the GDPR for technical innovations like big data analysis, by relaxing data minimisation and purpose specification requirements, is seen to be reflected in the German Adaptation and Implementation Act. The German rapporteurs note that, in several places, the Act weakens the rights of data subjects to the benefit of data controllers and processors, e.g. by adding an element of fault ('contributory negligence') to the risk-based liability regime of the GDPR or by eliminating the right to erasure in cases of high technical effort and low interest of the data subject.

The country reports show that, where the GDPR leaves a margin of manoeuvre, Member States adopt diverging solutions. The proposed Austrian Data Protection Amendment Act intends to lower the *age of consent of minors* to 14 years, whereas the Swedish report proposing a new Data Protection Act intends to lower it to 13 years. The Dutch draft Implementing Law provides that it applies to the processing of personal data in the context of activities of organisations in the Netherlands. This means that the criterion for applicability is the establishment of an organisation, not whether the fundamental rights of individuals in the Netherlands are affected; for instance, when services are offered on the internet from another Member State. According to the Dutch rapporteurs, the German Adaptation and Implementation Act takes the opposite view.

Besides legislative initiatives, rapporteurs (a.o. in Austria, Germany, Estonia, Italy, Greece, Hungary, Poland, Romania and Sweden) describe how their *DPAs* are issuing **guidelines** and offering online information tools to assist organisations in ensuring compliance. The Hungarian and Romanian country rapporteurs highlight that the guidelines adopted by the Article 29 Data Protection Working Party are very useful in this regard.

Only the German and Croatian rapporteurs refer to the need to address also national data retention rules in light of recent CJEU rulings,[136] in which the Court ruled that a general and indiscriminate data retention obligation might impose impermissible restriction of the fundamental rights and freedoms to personal data protection, privacy and freedom of expression (and annulled the Data Retention Directive). The Maltese rapporteur also mentions the ongoing discussions about the revision of the ePrivacy Directive/Regulation.

Non-EU Member States: Norway (which has a dualistic legal system) is transposing the GDPR through a national bill which is expected to enter into force simultaneously with the entry into force of the GDPR. The GDPR is considered not directly applicable in Switzerland, since the GDPR was neither designated as relevant under bilateral law nor notified to Switzerland as such[137] (contrary to Directive 1995/46/EC which is part of the bilateral acquis). By contrast, Directive (EU) 2016/680 ('Police Directive') is part of the Schengen acquis. The Schengen Association Agreement requires Switzerland to transpose the Directive. Switzerland is in the process of reforming its data protection legislation in order to align its rules with the modernised Council of Europe Convention No. 108, as well as with the GDPR (in the context of maintaining its equivalence decision as an EU third country and given that numerous Swiss companies will be directly affected by the provisions of the GDPR).[138]

Q4.2: How are businesses in your country adapting to the new requirements of the GDPR such as those related to consent, impact assessments, privacy by design and by default?

The reports generally state that businesses seem increasingly aware – albeit in varying levels depending on their size (see below) or the country concerned – of the need to review and adapt their internal processes to comply with the new requirements of the GDPR. In a Finnish survey, 90% of the larger businesses estimated that GDPR will have a significant impact on their business activities, mainly due to the strictly regulated conditions of consent, increasing compliance expenditures, new administrative sanctions, as well as the unpredictability of the new legal regime for data protection. The Italian rapporteur even states that the GDPR has *"prompted Italian businesses to pay unprecedented attention to data protection issues"* and notes that they gradually become aware that the GDPR's

[136] CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 and Watson*, 21 December 2016, ECLI:EU:C:2016:970, as well as Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, 8 April 2014, ECLI:EU:C:2014:238.

[137] This view is contested: the Federal Data Protection Supervisor (FDPIC), as well as part of the legal doctrine, considers the GDPR to be applicable even without formal adoption by Switzerland.

[138] For further details, see Swiss report, p.7-13.

obligations are not simply limited to additional paperwork (such as updating information notices). According to the Austrian, Czech, Estonian, Hungarian, Polish and Portuguese rapporteurs, official statistics or empirical data about the market impact of the GDPR are not available in their countries. Only in Finland a government funded survey into the attitudes and activities of businesses was carried out in 2017. Some rapporteurs (see e.g. France and Portugal) cite from surveys and studies carried out by commercial entities or industry associations, which attest globally that not all companies are ready.[139]

As the Croatian rapporteurs note, it is fair to say that the level of awareness regarding compliance with the GDPR corresponds to the size of enterprises, with large and international businesses usually actively preparing for the application of the GDPR, and awareness being (significantly) smaller amongst small and medium enterprises. This is also confirmed in a.o. the Czech and Spanish country reports. To address this awareness gap, *DPAs* in Belgium, Estonia, Croatia, Greece, the Netherlands, Malta, Poland, Romania, etc. are reported to be very active in educational activities and/or organising awareness activities (e.g. through publications in mainstream media channels or through start-up events).[140] But awareness is also, and perhaps most importantly, growing thanks to providers of *legal and consultancy* **services**. The large majority of rapporteurs note how such services have been booming in recent years. The private training market offers many new training courses in privacy and IT law, labelled "operational data protection", "IT compliance", "privacy governance" and targeting responsible employees of companies. Such courses are run by major publishers, law firms, job-related organizations and commercial providers, sometimes in cooperation with university teachers. The quality of the offers may vary depending on the organizer and they result in training certificates of varying reputation. In some countries, *accreditation mechanisms* are being set up to ensure a specific quality level (e.g. in Germany training certificates for the professional title "Specialist Lawyer Information Technology Law" must be recognized by the Bar Association).[141] All of the

[139] Note that the Polish rapporteur voices criticism on such commercial reports, as they are often authored by companies providing data security solutions, which, hence, have an interest in painting a rather bleak picture and showing a widespread lack of awareness. He notes that the accuracy, methodology and overall analytical value of those reports are questionable at best, and that the high demand for commercially offered GDPR trainings (see further below in the text) rather seems to indicate a significant level of awareness amongst businesses.

[140] Also various interest groups offer information (like check lists and "To Do" lists) about the GDPR, such as, for instance, the Austrian Federal Economic Chamber (WKO) and the Chamber of Labor.

[141] Although the activity of company data protection officer has a long tradition in Germany (contrary to e.g. Austria), there is currently no special qualification profile for the data protection officer. The task is usually carried out by lawyers, computer scientists or executives, predominantly members in large private specialized organizations.

larger law firms now have dedicated IT and privacy groups and see it as a growing business. Also *business associations* are providing their members with relevant information and develop appropriate best practices (see e.g. the Swiss report).

Concrete actions taken by *companies* include the carrying out of GDPR-specific compliance programmes; revision of data protection policies, procedures and controls; the introduction of procedures for data protection impact assessments; identification of gaps that need to be addressed; technical and organizational protection measures; the appointment of a Data Protection Officer; and the organisation of internal trainings to make staff aware of GDPR requirements. In Greece, new *insurance* packages are developed to protect companies from cybersecurity threats.

4.2. Internet of Things

Q4.3: What are the most contentious issues in your country (from a legal viewpoint) in relation to IoT (Internet of Things) / smart cities / Machine-to-machine generated data / automated cars? (Ownership issues? Access and use? Liability in case of harm?) Are there any specific legislative measures or regulatory opinions/ decisions in this area? What is the status of the policy debate?

The status of the discussions on IoT (Internet of Things), smart cities, Machine-to-machine generated data, and automated vehicles varies from country to country. The (academic and policy) debate is apparently very lively in countries like Austria, France, Germany, the Netherlands or Poland, but is still in its infancy in other countries, like the Czech Republic, Spain and Finland, or even (almost) non-existing, like in Croatia and Malta.

Recurring concerns in those debates relate to the *roles and liabilities of stakeholders; data ownership and use ('open data'); user privacy and data security; and transparency and safety issues* (e.g. hacking of poorly protected devices) *in IoT, smart cities, M2M communications, and automated cars*. Some country reports contain a detailed account of those ethical-legal discussions (see in particular the German, Dutch, Austrian, Swiss and Polish country reports; the Slovenian country report puts emphasis on its strict 'guarantist' approach to the right to personal data protection, as protected by its Constitution and interpreted by its Constitutional Court[142]) and touch upon challenging questions like: Should data generally be freely accessible to facilitate innovative solutions, or should it be protected

[142] Apparently, this strict interpretation was triggered by the "Affair udba.net"; see the Slovenian country report, p.39, with reference to B. Makarovič, "Foreign Internet content restriction in the Republic of Slovenia: Artificial borders within the Internet to protect personal data? ", *Journal of Computer, Media and Telecommunications Law*, 2003, Vol. 8, N° 5, p.371-374.

by – existing or to be created – proprietary rights? Under which circumstances should data obtained or specifically collected in the exercise of sovereign functions and using public funds be made available in the most conducive manner for the common good? Who is liable if a self-driving car causes an accident as a result of sudden acceleration? How to programme "crash optimization algorithms" to decide in dilemma situations where the system needs to choose between harming the driver or to people on the street?

In most countries, specific statutory laws and case law on these issues are still in an embryonic stage. As the Norwegian rapporteurs note; *"the law usually lags behind the technological development, making this area of law resemble a game of catch-up"*. Although a number of countries are in the process of adopting, or have adopted, *specific laws* (see below), the main source of legal innovation is, so the Norwegian rapporteurs argue, to be found in EU legislative measures. To illustrate, they refer to the 2015 Norwegian Law on Intelligent Transport Systems which was adopted to 'transpose' EU Regulations 885/2013, 886/2013 and 962/2015.

The Institutional Report indeed describes a wide array of initiatives recently adopted at EU level, dealing with various aspects of IoT, smart cities, etc. (think of the aforementioned draft ePrivacy Regulation, or the Commission's proposal for new rules on the *free flow of non-personal data* which was strongly supported by Estonia during its EU Presidency in the second half of 2017,[143] etc.).

More 'autonomous' national legislative initiatives (as the Norwegian rapporteurs call them) often relate to *autonomous motor vehicles (testing) and drones*: the Netherlands and Norway have recently adopted Acts on Autonomous Vehicles (Trials), while the German legislator last year amended its Road Traffic Act to regulate autonomous driving. Germany is very advanced in the discussions on automated vehicles. An interdisciplinary ethics committee on automated driving set up by the Federal Minister of Transport and Digital Infrastructure summarized its report in June 2017 in 20 theses.[144] The five key points are listed in the country report:

- Automated and connected driving is ethically required if the systems cause fewer accidents than human drivers (positive risk assessment).
- Property damage precedes personal injury: In dangerous situations, the protection of human life is always the highest priority.

[143] The Estonian rapporteurs stress that their country is a strong protagonist of digital and technological developments. Especially during its Council of the EU Presidency, Estonia has strongly promoted that, for the sake of a true data economy, data itself needs to become the fifth freedom of the EU. See e.g. the Estonian Vision Paper on the Free Movement of Data – the Fifth Freedom of the European Union, available at: https://www.eu2017.ee/sites/default/files/inline-files/EU2017_FMD_visionpaper.pdf .

[144] See https://www.bmvi.de/SharedDocs/EN/PressRelease/2017/084-ethic-commission-report-automated-driving.html.

- In the case of unavoidable accident situations, any qualification of persons for personal characteristics (age, gender, physical or mental constitution) is inadmissible.
- In every driving situation, it must be clear and identifiable who is responsible for the driving task: the human or the computer. Who drives, must be documented and stored (including to clarify possible liability issues).
- In principle, the driver must be able to decide himself on the passing on and use of his vehicle data (data sovereignty).

Also Portugal is studying the need to modify or broaden its existing rules on road traffic. Another area in which national legislators have adopted new rules concerns smart meters and smart electricity grids (e.g. the Austrian Electricity Economy and Organization Act 2010 was amended in 2017 to regulate the use of smart meters).

In some countries, the issues are not addressed yet through concrete legislative measures, but are being discussed in *strategy programmes or action plans*. Examples include the Hungarian overarching strategic document "Digital Success Programme 2.0" or the Czech National Action Plan for the Development of the Intelligent Transport Systems (ITS) until the Year 2020 (with an Outlook to the Year 2050) and the National Action Plan for the Smart Grid, adopted in 2015 by the Czech Ministry of Transport, respectively by the Ministry of Industry and Trade. The Czech rapporteurs also mention a couple of memoranda in which ministries are exploring legal issues relating to IoT and Industry 4.0 in general (discussing complexity and fragmentation of the legal framework; lack of interoperability standards, personal data processing, cybersecurity risks), or on automated cars (driver liability issues) and smart infrastructure.

France is discussing the need to introduce a *'robot law'* and specific *data ownership* regimes, as well as legal issues arising from (group) profiling. The Netherlands' Scientific Council for Government Policy (WRR) adopted a report in 2017 on *Big Data and Security Policies: Serving Security, Protecting Freedom*, in which it argues that the use of Big Data in the field of security requires a new regulatory framework, the emphasis of which should be on regulating data analysis and use, rather than on intensifying the regulation of data collection.

Ireland is presented by the Irish rapporteurs as a country of deeds and not words. There are several IoT projects and developments taking place (apparently, National Geographic recently cited Dublin as *"leapfrogging the competition in the race to be a smart city"*), but there is limited activity in terms of regulation and policy (apart from ComReg's Strategic Statement 2017-2019, in which it describes challenges arising from IoT for connectivity and numbering resources).

In a (limited) number of countries, *DPAs* have already adopted *guidelines* or *decisions relating to IoT, smart cities or autonomous driving.* The Spanish DPA

published guidelines on cloud computing in 2013 and a Code of Good Practice on Big Data in 2017. In the Greek report, we can read how the Hellenic Data Protection Authority has acted against the use of wearable location tracking devices designated for children, not only because of privacy risks but also to protect the moral and mental development of children. The use of location tracking devices may be used for children only for health reasons. Health treatment reasons have also been accepted by the Hellenic DPA to issue permissions to various communities to use smart devices equipped with GSM and GPRS systems and processing health data. Such smart devices are allowed to be used for social and health services offered from the communities to aged and handicapped people with their prior consent.

The Dutch report describes a couple of interesting smart city cases in which the DPA intervened. A first case relates to the use of *Wifi-tracking* technology in public-private partnerships and resulted in an order by the DPA subject to penalty payments on a company 'Bluetrace' that offered Wifi-tracking in and around shops.[145] The DPA found that the collection of personal data by means of Wifi-tracking can be necessary for legitimate business interest, but found, in this particular case, that the necessary guarantees — to protect the interests of data subjects outside the premises of retailers — were not in place. The authority requested, in particular, that adequate information be provided to the public about the fact that they are being registered by way of Wifi-tracking, and being tracked unnoticed via their mobile device. The Dutch DPA also intervened in a project by the municipality of Arnhem and requested that the collection of individual data by means of 'trash disposal cards' (afvalpas) be terminated because of its findings that the collection of personal data in this manner is not currently necessary for exercising public tasks.[146] In a press release dated 2 May 2017 regarding this matter, the DPA highlighted the importance of clarifying the purpose of data collection (in, e.g. tax collection), the importance of informing residents about this purpose and about the use of their data (which must be proportionate) and the need to adequately protect the 'trash disposal cards'.

The Swedish DPA has equally been active in several cases related to IoT, requiring for instance *health applications* to introduce stronger authentication mechanisms such as e-IDs[147] or one-time passwords. It has investigated complaints about alleged privacy breaches posed by the doll 'My Friend Cayla' and the intelligent robot 'i-Que'.[148] Although the Swedish DPA expressed concerns

[145] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-legt-wifi-tracker-bluetrace-last-onderdwangsom-op

[146] https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-gemeente-arnhem-past-afvalsysteem-aan

[147] The topic of eIDs is extensively discussed in the Swiss report (p.18-19).

[148] Also Germany and Norway have been confronted with similar complaints.

that these toys were breaching safety and personal integrity rules,[149] it found however that it lacked jurisdiction to review the complaint as the products were manufactured in China and the USA.[150]

Not only data protection authorities, but also some *competition authorities* and *communications regulators* are closely following up on developments in big data, IoT, etc. Both the Italian and Dutch rapporteurs describe such initiatives. In the Netherlands, the Authority for Consumer and Markets (ACM) is looking into M2M generated data since 2015, whereas in Italy, the Competition Authority (AGCM), the Communications Authority (AGCOM) and the Italian Data Protection Authority have opened on 30 May 2017 a joint Sector Inquiry on "Big data", with a view to identify potential competition concerns and define a regulatory framework able to foster competition in the markets of the digital economy, to protect privacy and consumers, and to promote pluralism within the digital ecosystem.[151]

4.3. Right To Be Forgotten

Q4.4: Since the CJEU's controversial judgment in May 2014 in the Google Spain (or Costeja) case, the so-called 'right to be forgotten' (or to 'delisting' or 'de-referencing') has received a lot of attention in Europe and beyond.[152] What is the legal status in your country? Are complaints being brought before the data protection authority and/or courts? Has there been a growing body of case law in this regard? How is the balance struck between the individual's right to data protection and the other interests at stake (in particular the search engine's commercial freedom, the public's right to information and the author's right to free expression)?

From the country reports, we can learn that the CJEU's *Google Spain* ruling did not lead to legislative amendments at national level. All Member States have transposed Directive 95/46/EC and are bound by the CJEU's interpretation of that directive, so data subjects have the right to request the delisting of links

[149] In particular, the DPA noted that the toys in question made it possible to spy on children, provide disguised advertising, resell personal data to third parties and were subject to terms and conditions which could change at any time.

[150] Swedish DPA newsletter "Integritet i fokus" (1/2017): "*My friend Cayla-storebrors bäste vän?*" (March 2017, p. 6-8).

[151] AGCM decision of May 30, 2017, No. 26620, case IC53, *Big Data*; available from http://www.agcm.it/stampa/comunicati/8781-ic53-avviata-indagine-conoscitiva-sui-big-data.html. For more information, see the Italian country report or the press release by AGCM at http://www.agcm.it/en/newsroom/press-releases/2384-%E2%80%9Cdig-data%E2%80%9D-italian-regulators-open-a-sector-inquiry.html (or https://www.competitionpolicyinternational.com/wp-content/uploads/2017/09/CPI-Nazzini.pdf).

[152] CJEU, Case C-131/12, *Google Spain and Google Inc v. AEPD and Costeja*, 13 May 2014, ECLI:EU:C:2014:317.

that are excessive or no longer accurate or up-to-date, even when such right to delisting is not *expressis verbis* written into domestic legislation, as the Czech and Estonian rapporteurs explicitly mention. The outcome of *Google Spain* judgment is now reflected in Art. 17 (2) of the EU General Data Protection Regulation (GDPR) and thus as of 25 May 2018 uniformly applicable EU law. In Germany, the Federal Data Protection Act 2017 (BDSG 2017) has made additional clarifications in § 35.[153] Also the Swiss upcoming new Datenschutzgesetz ('E-DSG') will provide for more explicit provisions regarding deletion (compared to the current rules, which – according to the Swiss report – already implicitly contain a right to delist).[154]

Data subjects are expected to bring their request first before the company concerned (very often, but not necessarily, the search engine provider like Google, Microsoft or Yahoo).[155] When their request is unsuccessful, they can bring a claim before their national DPA, and ultimately before the court (or a Data Privacy Appeals Board, like in Norway). In some countries, data subjects file their complaint directly before the court. In Portugal, for instance, matters associated with the right to free expression and free speech, breach of privacy and other conducts which may be considered criminal offences are handled directly by the courts, and not by the National Data Protection Authority (CNPD – *Comissão Nacional de Proteção de Dados*). The Dutch rapporteurs note that their DPA acts as a 'mediator' in cases where the search engine operator – usually Google – denied a delisting request.

In cases involving Google, courts usually address their order to Google Inc. while rejecting claims against the local entity (like Google fr or Google Deutschland) on the grounds that the latter is not the data controller and not capable of carrying out a delisting order (see in particular the Dutch, French and German[156] country reports). The Maltese rapporteurs note that their Office of the Information and Data Protection Commissioner (IDPCO) either assists the data subject to lodge the complaint with the Irish DPA or forwards itself the

[153] Deletion is not required if statutory storage obligations exist (§ 35(3) BDSG 2017). Instead of deletion, a restriction of processing pursuant to Art. 18 GDPR should occur if the controller has reason to believe that the interests of the data subject deserving protection would be violated (§ 35(2) BDSG 2017).

[154] Entwurf zum Datenschutzgesetz (E-DSG); see https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-68130.html. With regard to data processing by private persons, this is done by reference to the claims for the protection of the personality in accordance with Art. 28, 28a as well as 28g-28l of the Civil Code (Article 28 (2) (c) E-DSG). The E-DSG also addresses deletion of data from deceased persons.

[155] This is noted explicitly in the Estonian, Spanish and Greek country reports.

[156] Although the German rapporteur notes one recent decision (from 2017) by the Landesgericht Frankfurt in which Google Germany was ordered to delete the links concerned.

complaint, since it considers itself not competent to deal with the request as Google does not have any legal presence or establishment in Malta.

Whereas DPAs generally follow the *guidelines* issued in November 2014 by the *Article 29 Data Protection Working Party*,[157] some DPAs have issued their own recommendations or guidelines, e.g. in the Czech Republic and in Hungary.

Statistics about the number of (successful and rejected) delisting requests to Google are available from its Transparency Report (which contains, since February 2018, also details on categories of websites affected, of requesters, and of content targeted); also Microsoft provides statistics for its Bing search engine.[158] Statistics about cases brought before DPAs or courts are generally not available, but various rapporteurs signal an increase in cases involving the "right to be forgotten" in recent years, based on information from their DPA's annual reports or received after inquiry (e.g. in France, Estonia, Hungary, Italy, the Netherlands, Norway, Portugal, Romania and Sweden). The country reports contain a rich body of analysis on those cases (which may deal, for instance, with requests to delist links to information about previous convictions[159]).[160]

What transpires from the reports is that decisions always involve a *case-by-case assessment*, taking due account of the underlying facts. The Swedish country report is illustrative in this regard, where it discusses several disputes over individuals' requests to delist links to webpages containing accusations of fraud or (sexual) abuse. Depending on whether the individual held a *public role*,[161] had been given a *right to deny* the accusations in the publications concerned, and the *length of time* passed since the occurrence of the alleged behaviour, the data subject's complaint was upheld or rejected by the DPA or court. The Italian rapporteurs note that precedents in their country do not yet demonstrate a clear rule regarding the criteria for striking the balance between the individual's right to

[157] Guidelines of the WP29 on the Implementation of the *Costeja* ruling (26 November 2014).

[158] https://transparencyreport.google.com/eu-privacy/overview, respectively https://www.microsoft.com/en-us/about/corporate-responsibility/crrr. On 26 February 2018, Google released a research paper in which its statistics are further analysed: T. Bertram et al. (2018). "Three years of the Right to be Forgotten"; available from https://drive.google.com/file/d/1H4MKNwf5MgeztG7OnJRnl3ym3gIT3HUK/view

[159] For instance in Greece (Decision 83/2016 of the IDPA) and Norway (Decision no 10/2016 of the Data Privacy Appeals Board. In both cases the authorities found Google's refusal to delist unjustified, granting the complainant a 'digital right of redemption'. Also the Helsinki Administrative Court ordered Google on 8 December 2016 to remove access to two links in search results for a person's name, containing medical information in addition to information about the person's previous criminal activities, giving priority to the person's right to privacy over the public's right to information.

[160] In addition to the country reports, see also: https://blogdroiteuropeen.com/2017/06/15/revoir-les-20-contributions-de-notre-e-conference-sur-le-droit-a-loubli/.

[161] The Greek report notes that its DPA gives a broad interpretation of "public figure", including also members of a regulated profession (like doctors) when acting as professionals (Decision 83/2016).

data protection and the other interests at stake. Rather, Italian authorities have adopted a case-by-case approach, mostly taking into account the gravity of the facts relating to the data subjects, on the one hand, and the length of the time that has passed since the occurrence of such facts, on the other hand.

Nevertheless, several *criteria and principles* are consistently followed by DPAs and courts when assessing delisting requests and a number of country reports offer a systematic overview of those criteria. When discussing the *Mark Savage* case, which involved a former local election candidate who requested the removal from Google's search results of a link to the website 'Reddit.com' referring to him as *"North County Dublin's homophobic candidate"*, the Irish country report lists the following criteria which were taken into consideration by the Data Protection Commissioner (DPC):

- Is the data subject a public figure?
- Is the data accurate?
- Is the data relevant and not excessive?
- Is it clear that the data reflects an individual's personal opinion, or does it appear to be verified fact?
- In what context was the information published? Was the content voluntarily made public by the data subject?

At the same time, however, this case illustrates how the interpretation of these criteria in practice might diverge: whereas the DPC supported Google's refusal to remove the link, stating that the public interest and freedom of expression outweighed Mr. Savage's right to privacy, the Dublin Circuit Civil Court reached the opposite conclusion in May 2016. Appeal is pending before the High Court.

The Spanish country report equally lists various principles that can be derived from disputes before the DPA and courts, such as the need for data subjects to file their request before the right corporation (which is relevant in the case of multinationals like Google, Microsoft, Yahoo, etc.) and the duty for search engines to justify their decision (not) to delist information based on its relevance. The Spanish DPA has clarified that the relevance of the information should not be assessed at the moment when it was published or linked, but at the moment of the delisting request (information about how a professional provided a service is, for instance, no longer relevant when the individual ceased to provide that service). In case search engines wish to include some form of announcement when removing links, such *notification* should appear as a general message and not in relation to specific searches. Finally, the Spanish report highlights the relevance to distinguish between requests addressed to *search engines* and requests to

publishers.[162] In a decision of 2016, the Spanish DPA supports requests to eliminate metadata ("technical signals used by the newspaper to automatically communicate with the search engine, so that the information is not displayed by search engines"), rather than requiring the elimination of the information in the original source. This view had been put forward earlier by the Spanish Supreme Court.

The need for a differential treatment of general search engines and *newspapers' online archives* is also touched upon in the French (see below), Italian, Norwegian and Polish reports. In 2014, the Norwegian Data Privacy Appeals Board rejected a request by an individual that the publisher *Schibsted* should delete a number of old articles in its (online) newspapers. Although the complainant referred to the (at that time recently adopted) *Google Spain* ruling, the Board did not discuss *Google Spain* at all. It merely stated that the articles had a *journalistic purpose*, and thus were covered by the *right of freedom of speech*. In Poland, newspaper's websites are apparently not considered to be a collection of personal data, so individuals cannot act on the basis of the Personal Data Protection Act, but instead have to invoke civil law remedies, based on personality rights in the Civil Code. Interestingly, the Polish rapporteur refers to the *Węgrzynowski and Smolczewski v. Poland* ruling of the European Court of Human Rights, in which the Court upheld the Polish courts' refusal to grant an order against a newspaper for the removal of a defamatory article from its website, underlining that "it is not the role of judicial authorities to engage in rewriting history *by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations.*"[163]

Italian courts seem to be more divided over the issue. In relation to information that was factually correct but outdated, the Italian *Corte di Cassazione* held in 2016 that an online newspaper had to erase information from its archive because, notwithstanding the de-listing, the information was easily accessible to the public.[164] Conversely, in its judgment of January 2017, the Court of Rome held that the right to de-listing does *not* include the right to have information

[162] Press publishers, press councils and journalists' associations often have already a strong tradition of developing guidelines on the 'right to be forgotten'. See, for instance, the example of the Swiss Press Council and the Swiss Code of Journalists (Declaration of the Obligations and Rights of Journalists), described in the Swiss report (p.21).

[163] ECtHR, 16 July 2013, *Węgrzynowski and Smolczewski v. Poland*, http://hudoc.echr.coe.int/eng?i=001-122365.

[164] Also the Belgian Court of Cassation upheld the judgment of the Court of Appeal of Liège which ruled that the publisher who, after notification by a natural person, had refrained from anonymizing certain articles containing information about the judicial history of the person, could, in certain circumstances, be held liable for damages; Court of Cassation (BE), 29 April 2016, C.15.0052.F; available from https://inforrm.files.wordpress.com/2016/07/ph-v-og.pdf

erased from the archive of an online newspaper, which provides news access to those who are specifically seeking out that information.

In relation to this, it can be noted that Dutch courts have in a number of cases not only considered the search engine operator's economic interests, but also its *right to freedom of information*, the important role of search engines in facilitating access to online information, and the need for courts to exercise restraint in imposing restrictions on their activities so as to protect their catalogue function. In a recent ruling regarding a delisting request, related to a lawyer's conviction for a knife crime, the Court of Appeals of the Hague held that a search engine operator can potentially rely on the journalistic exemption, and that there is still room to consider the right to freedom of expression if search engine operators process sensitive data.

The Estonian rapporteurs state that, in general, a data subject does not have a 'right to be forgotten' or to have data deleted, if there exists a legal ground for this data to be processed in a lawful way. There exists, for instance, no right to have your data deleted in public registers, like a population register. That is, unless not all personal data in that register is relevant for the objective pursued by the register, as the Croatian rapporteurs explain. Recently, the Croatian DPA ordered that personal data of government officials on their marital status or number of children had to be removed from the registry set up pursuant to the Act on Prevention of the Conflict of Interest, since such information was not considered relevant to understand whether the official is in a conflict of interest. Moreover, the fact that a legal obligation exists to publish certain data on government portals does not necessarily imply a right to re-use that data on other sites or in other services (as the *Satamedia* case made clear),[165] or to include links to that information in general search engines. The Hamburg Data Protection Supervisor, for instance, recently found (in 2017) that Google Inc. is not allowed to link to personal data resulting from consumer insolvency proceedings. Such information is publicly accessible electronically on the government portal, but is protected from systematic access by search engines by robots.txt files. This is intended to ensure that privately owned persons do not suffer permanent damage or are specifically exposed to marketing measures.[166]

[165] The case involved the re-use of (personal) tax data collected by private companies from documents in the public domain held by tax authorities for publication in a newspaper and for commercial distribution via CD-ROMs and a SMS service. The legal dispute before the Finnish courts led to judgments of both the CJEU and the ECtHR (in Grand Chamber) endorsing the national courts' narrow interpretation of 'journalistic exception' in the data protection legislation: CJEU, Case C-73/07, *Satamedia*, 16 December 2008, ECLI:EU:C:2008:727 and ECtHR, *Satamedia v. Finland*, 27 June 2017, http://hudoc.echr.coe.int/eng?i=001-175121.

[166] A comparable case about insolvency data is discussed in the Austrian country report, together with two cases about the 'auto-complete' function of Google's search engine.

In the Netherlands, Germany and in France, a particularly rich body of case law on the 'right to be forgotten' has emerged. According to its rapporteurs, France is the country with most delisting requests (130,536 requests, 48.7% of URLs deleted as of July 12, 2017).[167] A first series of disputes in France relates to refusals by Google to delist certain URLs in response to an applicant's request. In most cases, the High Court (Tribunal de Grande Instance) found the refusal not justified by the public's right to legitimate information. In a second series of cases, the request was addressed to a newspaper for removal of links from the internal search engine of their online archives. In those cases, the courts (and in particular the Court of Cassation) considered that the freedom of the press opposes the existence of an obligation for the press to delist links in their online archives, or to anonymise all personal data in those archives.

Recently, the French Council of State *(Conseil d'État)* referred two *preliminary questions to the CJEU*, one concerning the scope of the delisting obligation for search engines with regard to *sensitive data* relating to criminal convictions or security measures,[168] the other in relation to the *geographical scope* of the right to be forgotten.[169] Both issues have been the topic of legal discussions in other Member States as well, sometimes resulting in conflicting rulings by lower courts (see in particular the Dutch country report on the issue of processing sensitive data).[170] The outcome of the procedures before the CJEU is therefore awaited by DPAs and courts all over Europe (and beyond).

[167] This is confirmed in the paper by T. Bertram et al. (2018). "Three years of the Right to be Forgotten", p.6; available from https://drive.google.com/file/d/1H4MKNwf5MgeztG7OnJRnl3ym3gIT3HUK/view. According to the latest figures in Google's Transparency Report (31 March 2018), France generated 144,746 requests to delist a total of 502,307 URLs (compare with the figures for the n°2 and n°3 countries: 110,854 requests for 417,032 URLs in Germany and 80,732 requests for 323,412 URLs in the UK). When looking at URLs requested for delisting *per capita* (both population and internet-using population), Estonia is the leading country, whereas the Czech Republic has the highest delisting rate of requested URLs (meaning that Czech requesters are most successful; cf. T. Bertram et al. (2018), p.6). In total, 664,714 URL removal requests (for 2,466,205 URLs) have been made worldwide (mainly affecting social networks and forums, like Facebook, Youtube and Google+, and directory services, such as profileengine.com and annuaire.118712.fr).

[168] More information: http://english.conseil-etat.fr/Activities/Press-releases/Right-to-be-delisted (Conseil d'Etat) and https://www.blog.google/topics/google-europe/defending-access-lawful-information-europes-highest-court/ (Google blog). Also: http://www.zdnet.com/article/google-right-to-be-forgotten-case-goes-to-top-eu-court/.

[169] Request for a preliminary ruling from the Conseil d'État (France) lodged on 21 August 2017 – Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), Case C-507/17.

[170] In Greece, Decision 82/2016 of the DPA concerned delisting of links from both google.gr and google.com but only for individuals using those search engines from Greece. Dutch courts seem to apply the same approach, focusing on search results where Google search is accessed from the Netherlands, or on EU versions of Google search. In line with the position of the French *CNIL* and the WP29 Guidelines, the Swedish DPA argued for a 'right to be forgotten' which extends beyond EU domains in its decision of 2

We end this report with some good advice from the German consumer protection association *Verbraucherzentrale*: internet users should regularly engage in *egosurfing* or *self-googling* (*i.e.* search for themselves) and ask the search engine providers for the deletion if information is out of date!

May 2017 in case 1013-2015. In particular, the Authority found that the Swedish Personal Data Act could, under certain conditions, apply to Google' search results, even if these were provided outside Sweden. The DPA ordered therefore Google to delist search results from foreign domains (such as google.com) if those results have such a 'special connection' to Sweden and to the data subject that they would violate his or her personal integrity. As examples of a 'special connection', the Swedish DPA mentions search results linking to websites in Swedish or directed to a Swedish audience. Compare with the Supreme Court of Canada which upheld a global delisting obligation for Google on June 28, 2017 in *Google Inc. v. Equustek Solutions Inc.;* for more information, see: https://globalfreedomofexpression.columbia.edu/cases/equustek-solutions-inc-v-jack-2/ (but note that, in November 2017, the District Court for the Northern District of California granted Google's motion for preliminary injunctive relief stating that the Canadian court's order to delist Datalink search results globally cannot be enforced in the United States).

INSTITUTIONAL REPORT



INSTITUTIONAL REPORT

Piedade Costa de Oliveira*

Introduction

It is common ground that the EU internal market is heavily impacted by the unprecedented changes brought by technological developments in information and communication technologies (ICT). This phenomenon predates the current century but has accelerated in the last decade. As a matter of fact, digital technologies are increasingly powering the exchange of goods and services at national level and across borders. They are changing production processes in industry as well as bringing new actors to traditional sectors and, at the same time, challenging existing market operators and practices. Also, internet based businesses attract consumers but the latter are afraid of the lack of protection. Similarly, businesses, in particular SME's are eager to benefit from the opportunities offered by electronic commerce but fear the difficulties and costs of compliance with different legal systems. In this context, with digitisation advancing, adapting single market rules becomes increasingly important to ensure its functioning. Furthermore, whereas the internet attracts people and has been considered as having the potential of empowering and liberating, at the same time it has the potential of being abused by criminals. Furthermore, recent trends are emerging, showing the internet as a battleground of interests in which the very foundations of democracy are perceived as being endangered by manipulation and disinformation. In addition, the rise of Internet of Things (IoT) and with it artificial intelligence and increased use of automated and algorithmic deci-

* Member of the Legal Service of the European Commission. The views presented in this report are those of the author alone and do not represent an official position of the European Commission.

sion-making challenges the adequacy of existing legal frameworks[1] to ensure that artificial intelligence is developed and used in line with the fundamental rights, values and principles that form the foundation of our democracies. This requires understanding of the technical aspects of artificial intelligence, of its socio-economic impact, as well as of its consequences on the rule of law, fundamental rights and democracy.

In this report we will start by presenting the historical developments of the Digital Single Market. Then we will present a summary of a selection of actions undertaken by the Commission following the adoption of its Digital Single Market Strategy of 2015. In this respect, we will focus on legislative proposals. In section 2 we will deal with the e-Commerce Directive and the developments of the case-law in this regard. Finally, in section 3, we will present the main novelties of the new rules on the protection of personal data and present a brief summary of selected recent court cases.

1. The Digital Single Market

1.1. Historical developments

With the development of personal computers in the 80's and 90's, the European Union adopted various acts, mainly directives, in certain fields such as intellectual property[2], data protection[3] and telecommunications[4] aimed at addressing

[1] E.g. the adequacy of the Product Liability Directive (85/374/EEC, as amended by Directive 1999/34/EC). The Commission launched a public consultation on 12 September 2016 with a deadline for replies until 26 April 2017. The aim of this consultation is to collect stakeholders' feedback on the application and performance of the Directive, including on how it relates to challenges raised by new technological developments, notably in cases of damage caused by new technologies, such as robots, automated systems, or complex IoT products.

[2] Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property, OJ L 346, 27.11.1992, p. 61; Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights, OJ L 290, 24.11.1993, p. 9; Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, OJ L 248, 6.10.1993, p. 15; Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, p. 20.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31; Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24, 30.1.1998, p. 1.

[4] Directive 97/13/EC of the European Parliament and of the Council of 10 April 1997 on a common framework for general authorizations and individual licences in the field of telecommunications services, OJ L 117, 7.5.1997, p. 15; Directive 97/33/EC of the European Parliament and of the Council of 30 June 1997 on interconnection in Telecommunications with regard to ensuring universal service and interoperability through application of the principles of Open Network Provision (ONP), OJ L 199, 26.7.1997, p. 32.

certain problems concerning the functioning of the internal market brought about by new technologies. With its Communication of 1997 'A European Initiative on Electronic Commerce'[5], the Commission presented its view on a coherent approach to encourage the growth of e-commerce it considered as a field crucial for Europe's competitiveness on world markets. To that effect, the Commission proposed a comprehensive set of actions that framed the EU's subsequent approach to the internet. The Communication states that regulatory responses need to be addressed at every step of the business activity, from the establishment of business, to the promotion and provision of electronic commerce activities, through conclusion of contracts, to the making of electronic payments. It adds that in parallel, a number of key 'horizontal' issues affecting the entire electronic commerce activity, need to be addressed. These include data security, protection of intellectual property rights and conditional access services, privacy, as well as a clear and neutral tax environment. Four principles were considered to provide an 'adaptable and appropriate framework for legislation', each of them accompanied by a brief explanation (cf. para. 39). These four principles are the following: *No regulation for regulation's sake; Any regulation must be based on all Single Market freedoms; Any regulation must take account of business realities; Any regulation must meet general interest objectives effectively and efficiently;*

In 1999, a new step was taken with the Lisbon Declaration and the Commission Communication 'e-Europe – An Information Society for All'[6], with the aim to make Europe the most dynamic 'knowledge-based economy in the world' by 2020 (Europe 2020). Following that, a number of actions were initiated and directives adopted, such as a new telecommunications framework and the e-Commerce Directive (2000/31/EC[7]).

A new Communication ('A Digital Agenda for Europe')[8] was adopted on 19 May 2010. It states that '[T]he Digital Agenda for Europe is one of the seven flagship initiatives of the Europe 2020 Strategy, set out to define the key enabling role that the use of ICT will have to play if Europe wants to succeed in its ambitions for 2020'. Its objectives are to chart a course to maximise the social and economic potential of ICT, most notably the internet, considered a vital medium of economic and societal activity for doing business, working, playing, communicating and expressing ourselves freely. The Communication sets out an action plan aiming, among others, at increasing access to fast internet, improving trust and

[5] COM(97) 157 final.

[6] COM(1999) 687 final.

[7] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, 17.7.2000, p. 1.

[8] COM(2010) 245 final.

security and improving research and innovation. Among the key actions identified in its Annex, it is worth flagging two of them given their horizontal nature and importance for the functioning of the Digital Single Market:

(i) the review of Directive 95/46/EC on the protection of personal data[9] , to enhance individuals' confidence and strengthening their rights (Key action 4). The proposal was presented early 2012 and Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR)[10] was adopted in 2016. It will become applicable from 25 May 2018.

(ii) the review of Directive 1999/93/EC on a Community framework for electronic signatures to ensure cross-border recognition and interoperability of secure eAuthentication systems (Key Action 3). A proposal for a Regulation was also presented in 2012, followed by the adoption of Regulation 910/2014 on electronic identification (eIdentification) in 2014[11]. This Regulation is applicable since 1 July 2016.

1.2. The 'Digital Single Market Strategy for Europe'

On 6 May 2015 the Commission presented the *'Digital Single Market Strategy for Europe'*[12], identified as one of its key priorities. The Communication sets out the Commission's vision on how to address the major challenges brought about by the rapid developments of the internet and digital technologies that are transforming all aspects of individuals' lives, the society and the economy. The Communication states that:

> "A Digital Single Market is one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. Achieving a Digital Single Market will ensure that Europe maintains its position as a world leader in the digital economy, helping European companies to grow globally."

The Commission's approach is to focus on key interdependent actions, to be taken at EU level, aiming at bringing down barriers that have or are developing in

[9] OJ L 281, 23.11.1995, p. 31.

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1 (GDPR)

[11] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73.

[12] COM(2015) 192 final.

the digital market. All of the actions envisaged by the Commission are intended to address new challenges brought by rapid technological developments and globalisation. They should all work together in a complementary manner and, in the Commission's view they can only achieve in full the growth objectives if they are all adopted. The expected benefits are (i) new opportunities for businesses to scale up across the single market, (ii) foster better services at better prices and offer more choice for consumers, (iii) create new sources of employment.

To achieve those aims, the Commission has chosen different actions, such as, reviewing and updating existing legal instruments by amending them, proposing new targeted legal instruments in certain other areas; clarifying existing rules through guidance and fostering research in new and emerging technologies. The fields of action are summarised in the following three pillars identified in the Digital Single Market Strategy. Under each of them, the Commission has put forward different initiatives, a selection of which is summarised below together with most recent developments of the legislative process, where applicable.

Pillar 1: Better access for consumers and businesses to online goods and services across Europe – this requires the rapid removal of key differences between the online and offline worlds to break down barriers to cross-border online activity.

On December 2015, the Commission put forward the *Digital Contracts Package*, consisting of two proposals: a proposal for a Directive on certain aspects concerning contracts for the supply of digital content (*DCD*)[13] and a proposal for a Directive on certain aspects concerning contracts for the Sales of Goods (*sales of goods proposal*), as amended[14].

The *DCD* proposal aims to fully harmonise the key contract law rules for the supply of digital content, such as the legal remedies for failure to supply the digital content or for non-conformity of the digital content with the contract, the legal guarantee period as well as rules on termination of contracts. This proposal covers contracts in cases where the consumer pays a price but also where the consumer does not pay a price but actively provides personal data or any other data.

[13] COM(2015) 634 final.

[14] COM (2015)635 final. In October 2017 the Commission adopted the amended proposal for a Directive on certain aspects concerning contracts for the sales of goods, which extends the scope of the proposal of a Directive on certain aspects of contracts for the online and other sales of goods (Online Sales of Goods proposal) to all consumer sales (COM(2017) 637 final).

The initial proposal for *sales of goods* covered only online and other distance sales. Subsequently, it was amended[15] by the Commission in order to take into account the discussions in the European Parliament and in the Council, during which the co-legislators have stressed the need to have coherent rules for distance and face-to-face sales of goods. The amended proposal therefore extends its scope to all contracts of sales of goods concluded between a seller and a consumer. The intention is to fully harmonise rules on conformity requirements, remedies available to consumers for lack of conformity of the goods with the contract and modalities for their exercise and to increase the level of consumer protection as compared to Directive 1999/44/EC on consumer sales and guarantees which only *provides for minimum harmonisation*.

Both the DCD and the *of goods* proposals aim to contribute to fostering growth through the creation of a true Digital Single Market, to the benefit of both consumers and businesses, by eliminating the key contract law-related real or perceived barriers hindering cross-border trade. In this respect, recital 9 of the amended proposal on the sales of goods states that 'fully harmonised consumer contract law rules will make it easier for traders to offer their products in other Member States. Businesses will have reduced costs as they will no longer need to take account of different consumer mandatory rules. They will enjoy more legal certainty when selling at a distance to other Member States through a stable contract law environment.'

Legislative work on the *DCD* proposal is advancing faster than on the sales of goods proposal. Indeed, the Council adopted its General Approach (GA) on 8 June 2017. The European Parliament defined its negotiating position for trilogues on 21 November 2017. Interinstitutional negotiations started in December 2017.

Another proposal was presented in December 2015, for a *Regulation on cross-border portability of online content services*[16]. The Regulation, adopted on 14 June 2017[17], will be applicable from 20 March 2018. It will enable consumers to access their online subscriptions such as music, games, films, entertainment programmes or sports events when travelling in other Member States. Its main objective is to provide a common approach to the provision of online content services to subscribers temporarily present in a Member State other than their Member State of residence by removing barriers to cross-border portability of online content services which are lawfully provided.

[15] In October 2017 the Commission adopted the amended proposal for a Directive on certain aspects concerning contracts for the sales of goods, which extends the scope of the proposal of a Directive (COM (2015)635) on certain aspects of contracts for the online and other sales of goods (Online Sales of Goods proposal) to all consumer sales (COM (2017) 637 final).

[16] COM(2015) 627 final.

[17] Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market, OJ L 168, 30.6.2017, p. 1.

On 25 May 2016[18], the Commission presented another set of legislative proposals: a proposal on banning unjustified *Geoblocking*[19], a proposal for the revision of the *Audiovisual Media Services Directive (AVMSD)*[20] and a proposal for a new *Consumer Protection Cooperation (CPC) Regulation*[21].

Geo-blocking can be described as a method that companies use to make sure that only those persons in a specific geographic location are able to access a certain website and the goods or services offered through that website. That website recognises a person's location for instance by checking the device's IP address, payment means to be used or the person's postal address. Persons trying to access the website from other locations than the ones selected by the company may either simply be blocked or be diverted to another website, where the relevant conditions for obtaining the goods or services in question (notably: prices) may differ. Where there is no objective justification for such differential treatment, it is considered a discriminatory practice that prevents online customers from accessing and purchasing products or services from a website based in another Member State. The Explanatory Memorandum accompanying the proposal states that its general objective is to give customers better access to goods and services in the Single Market by preventing direct and indirect discrimination by traders artificially segmenting the market based on customers' residence. Customers experience such differences in treatment when purchasing online, but also when travelling to other Member States to buy goods or services in offline situations.

The interinstitutional negotiations resulted in a political agreement between co-legislators and the Commission on the draft Regulation, on 20 November 2017. Once adopted, it will prohibit discrimination based on customer's nationality, place of residence or place of establishment in the situations covered.

It should be noted that these new rules on geo-blocking do not cover the provision of certain online content to which a consumer subscribes. This matter is covered by the abovementioned regulation on cross-border portability of online content services.

[18] For more information on measures put forward by the Commission on 25 May 2016, including on the Commission's guidance on unfair commercial practices Directive, see: http://ec.europa.eu/consumers/enforcement/cross-border_enforcement_cooperation/index_en.htm

[19] Proposal for a Regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC, (COM(2016)289 final).

[20] COM(2016)287 final: Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), OJ L 95, 15.4.2010, p. 1.

[21] COM(2016) 283 final.

The proposal for a revision of *AVMSD* maintains the minimum harmonisation approach and the country of origin principle for media service providers. The main new elements are the prohibition of hate speech, better protection of minors, notably, through the reinforcement of the requirements applicable to on-demand services and the extension of its scope to include video-sharing platforms, the promotion of European works, accessibility of audio-visual content and the reinforcement of the independence of regulators.

Concerning the protection of minors and incitement to hatred, the proposed changes mean that platforms which organise and tag a large quantity of videos should protect minors from harmful content and protect all citizens from incitement to hatred, based on new EU-specific terms. Concerning the prohibition of hate speech, the grounds for prohibition should be aligned to those of the Framework Decision on combating certain forms and expressions of racism and xenophobia, as defined in Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law[22]. The most harmful content should be subject to the strictest measures, such as PIN codes and encryption.

At the time of writing, this proposal went through several interinstiutional meetings between the co-legislators and the Commission (trilogues). However, no agreement has been reached yet.

The proposal for a new *CPC Regulation*[23], that will replace current Regulation 2006/2004[24], addresses the need to better enforce EU consumer law, especially in the fast evolving digital sphere. Its general objective is to develop modern, efficient and effective CPC mechanisms that will reduce the consumer detriment caused by cross-border and widespread infringements to Union consumer law. This includes in particular reducing situations where important cross-border and widespread infringements are not detected or sufficiently addressed through the CPC framework and ensuring that consumer protection authorities reach similar outcomes regarding the same malpractices. The level of harmonisation is deepened in order to address the above issues and to boost the cross-border enforcement of Union consumer laws in the Single Market. The New Regulation was adopted on 12 December 2017[25] and will apply from 17 January 2020.

[22] OJ L328, 6.12.2008, p. 55.

[23] COM(2016) 283 final.

[24] Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation), OJ L 364, 9.12.2004, p. 1

[25] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (OJ L 345, 27.12.2017, p. 1).

Another important measure for the functioning of the Digital Single Market is the proposal *on copyright in the Digital Single Market*[26], presented on 14 September 2016. Recital 3 states that, '[r]apid technological developments continue to transform the way works and other subject-matter are created, produced, distributed and exploited. New business models and new actors continue to emerge. The objectives and the principles laid down by the Union copyright framework remain sound. However, legal uncertainty remains, for both rightholders and users, as regards certain uses, including cross-border uses, of works and other subject-matter in the digital environment.' The fourth title of the proposal concerns measures to achieve a well-functioning marketplace for copyright. In particular, Article 13 should be signalled. It creates an obligation on information society service providers storing and giving access to large amounts of works and other subject-matter uploaded by their users to take appropriate and proportionate measures to ensure the functioning of agreements concluded with rightholders and to prevent the availability on their services of content identified by rightholders in cooperation with the service providers (see also recital 38)[27]. This proposal is in the legislative process.

On 1 December 2016 the Commission presented three proposals[28] aimed at modernising the current VAT rules that apply to e-commerce activities and

[26] COM(2016) 593 final.

[27] Recital 38 reads as follows: 'Where information society service providers store and provide access to the public to copyright protected works or other subject-matter uploaded by their users, thereby going beyond the mere provision of physical facilities and performing an act of communication to the public, they are obliged to conclude licensing agreements with rightholders, unless they are eligible for the liability exemption provided in Article 14 of Directive 2000/31/EC [...]
In respect of Article 14, it is necessary to verify whether the service provider plays an active role, including by optimising the presentation of the uploaded works or subject-matter or promoting them, irrespective of the nature of the means used therefor.
In order to ensure the functioning of any licensing agreement, information society service providers storing and providing access to the public to large amounts of copyright protected works or other subject-matter uploaded by their users should take appropriate and proportionate measures to ensure protection of works or other subject-matter, such as implementing effective technologies. This obligation should also apply when the information society service providers are eligible for the liability exemption provided in Article 14 of Directive 2000/31/EC.'

[28] Proposal for a Council Regulation amending Regulation (EU) N° 904/2010 on administrative cooperation and combating fraud in the field of value added tax (COM(2016) 755 final); proposal for a Council implementing Regulation amending Implementing Regulation (EU) No 282/2011 laying down implementing measures for Directive 2006/112/EC on the common system of value added tax (COM(2016) 756 final); proposal for a Council Directive amending directive 2006/112/EC and Directive 2009/132/EC as regards certain value added tax obligations for supplies of services and distance sales of goods (COM(2016) 757 final),

helping making VAT future-proof. The reasons to act put forward by the Commission were, in essence, the following[29]:

'First, the complexity of VAT obligations has consistently been identified as one of the key reasons why a business will not engage in cross-border e-commerce, and therefore it means that the single market cannot be accessed by many businesses especially SME's. [...]

Second, the current system is not neutral as EU businesses are at a clear disadvantage to non-EU businesses which can legitimately and through high levels of non-compliance make VAT-free supplies into the EU. Given that VAT rates can be as high as 27%, there is a substantial distortion in favour of non-EU business if VAT is not applied even providing an incentive for EU businesses to delocalise outside the EU..

Third, the complexity of the existing system as well as the current exemption for the importation of small consignments means that Member States lose valuable tax revenues. It is estimated that due to the VAT exemption of the importation of low value small consignments and the undervaluation of the imported goods such VAT losses are currently as high as EUR 5 billion annually.'

Among the objectives of the proposal for new VAT rules there are: (i) the extension of the current VAT one-stop shop (OSS) to all intra-EU B2C (business-to-consumer) supplies of goods and services. These rules already exist for supplies of telecommunication, broadcasting and electronic services supplied to consumers. The OSS is an electronic system that currently allows online companies established in the EU or in non-EU countries supplying such services to declare and pay VAT in a single Member State through a quarterly VAT return for all their sales to final consumers in the EU. That Member State then distributes the VAT amounts received between the Member States where telecommunication, broadcasting and e-services are bought and consumed; (ii) the removal of the existing distance sales thresholds of EUR 35.000 or 100.000 applicable per Member State to which supplies to consumers are made and replace this with the new EUR 10.000 threshold for all cross-border supplies of telecommunication, broadcasting and e-services as well as for distance sales in the EU and (iii) the removal of the VAT exemption for the importation of small consignments from outside the EU, whereby imported goods bought online from non-EU countries are exempt from VAT if they cost below EUR 22. Companies based within the EU or outside the EU can fraudulently mark expensive goods as costing less than EUR 22, meaning that no VAT is paid upon importation. This removal of the exemption for small consignments would ensure a level playing field with EU businesses supplying goods in the EU. Finally, another important element

[29] Cf. Explanatory Memorandum, COM(2016) 757 final.

contained in this package of measures is (iv) the increased liability of marketplaces that will become deemed suppliers when they intervene in the importation of goods with a value up to EUR 150 supplied to private consumers in the EU or when they facilitate the supply of goods already located within the EU but supplied to consumers in the EU by non-EU established suppliers..

The new Council Directive (EU) 2017/2455 amending Directive 2006/112/EC and Directive 2009/132/EC as regards certain value added tax obligations for supplies of services and distance sales of goods as well as the new Council Regulation (EU) 2017/2454 amending Regulation (EU) No 904/2010 on administrative cooperation and combating fraud in the field of value added tax were adopted on 5 December 2017[30]. These rules will enter into force in 2019 for improvements of the current 'Mini one-stop shop' and as of 2021 for the other parts.

Pillar 2: Creating the right environment and conditions for digital networks and services to flourish: this requires high-speed, secure and trustworthy infrastructures and content services, supported by the right regulatory conditions for innovation, investment, fair competition and a level playing field.

The actions undertaken by the Commission cover, *inter alia*, the overhaul of the telecom rules, the so-called connectivity package, presented on 14 September 2016[31], which includes a proposal for a *Directive establishing the European Electronic Communications Code (EECC)*[32], the new rule book for providers of internet access and communication services, but also a *Communication on connectivity*[33] setting out Common broadband targets and strategic objectives by 2025, a *5G Action Plan* setting out a roadmap for public and private investment on 5G infrastructure in the EU[34], and a *legislative initiative* aimed at bringing *free access to WIFI connectivity in public spaces like parks, libraries and squares (WIFI4EU).*

The *EECC* is a recast of the four Directives which form the current telecommunications regulatory framework[35], revised for the last time in 2009. As stated

[30] OJ L 348, 29.12.2017, pp. 7 and 1, respectively.

[31] https://ec.europa.eu/digital-single-market/en/right-environment-digital-networks-and-services

[32] COM(2016)590 final.

[33] COM(2016)587final.

[34] https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan

[35] Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) (OJ L 108, 24.4.2002, p. 7); Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) (OJ L 108, 24.4.2002, p. 21); Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24.4.2002, p. 33); Directive 2002/22/EC of the European

in the Explanatory Memorandum accompanying the proposal, the telecommunications sector has evolved significantly since 2009 and its role as an enabler of the online economy has grown. Market structures have changed and connectivity has become a widely pervasive feature of economic life. In particular, 'consumers and businesses are increasingly relying on data and internet access services instead of telephony and other traditional communication services. This evolution has brought formerly unknown types of market players to compete with traditional telecom operators (e.g. so called over-the-top -players (OTTs): service providers offering a wide variety of applications and services, including communications services, over the internet). At the same time, it has also increased the demand for high-quality fixed and wireless connectivity with the rise in the number and popularity of online content services, such as cloud computing, the Internet of Things, Machine-to-Machine communication (M2M) etc. [...] '. Furthermore, recital 15 explains that end-users increasingly substitute traditional voice telephony, text messages (SMS) and electronic mail conveyance services by functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services. In order to ensure that end-users are effectively and equally protected when using functionally equivalent services, a future-oriented definition of electronic communications services should not be purely based on technical parameters but rather build on a functional approach.

On the basis of the above, the Commission proposed as one of the novelties of the *EECC* that not only traditional telecom operators but also new actors, i.e. OTTs, should be submitted to the regulatory regime. Such new players should however only be subject to a light regulatory approach, meaning that they 'should be subject only to obligations, where public interests require applying specific regulatory obligations to all types of interpersonal communications services, regardless of whether they use numbers for the provision of their service' (see recital 18)..

At the time of writing, interinstitutional discussions are ongoing between the three institutions.

With its proposal on *WIFI4EU*[36] the Commission proposed amending the Connecting Europe Facility Regulation (CEF)[37] and the Regulation on guidelines

Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108 24.4.2002, p. 51).

[36] COM(2016) 589 final.

[37] Regulation (EU) No 1316/20136 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No 913/2010 and repealing Regulations (EC) No 680/2007 and (EC) No 67/2010, OJ L 348, 20.12.2013, p. 129, as last amended by Regulation (EU) 2015/1017 of the European Parliament and of the Council of 25 June 2015, OJ L 169, 1.7.2015, p. 1.

for trans-European networks in the area of telecommunications infrastructure[38], in view of increasing the financial envelope for the implementation of CEF by an amount of EUR 50 000 000. The Union would provide financial assistance, which should essentially take the form of grants, to projects of non-commercial character aimed at bringing free access to WIFI connectivity in public spaces like parks, libraries and squares. The Regulation was adopted on 25 October 2017[39]. Under this new legal instrument, local public authorities (municipalities or groups of municipalities) wishing to offer WIFI in areas where a similar public or private offer does not yet exist will be able to apply for funding via a simple and non-bureaucratic process. A grant allocated in the form of vouchers will be used to purchase and install state-of-the art equipment, i.e. local wireless access points, while the public authority will cover the running costs of the connection itself.

Pillar 3: Maximising the growth potential of our European Digital Economy – this requires investment in ICT infrastructures and technologies such as Cloud computing and Big Data, and research and innovation to boost industrial competiveness as well as better public services, inclusiveness and skills.

Under this pillar, the actions undertaken by the Commission cover essentially non-legislative initiatives, such as public private partnerships. They are all aimed at fostering research in certain areas such as *Cloud Computing, Big Data* and *cybersecurity,* strengthening the *digital skills* and literacy of the Union population and boosting the industrial competitiveness of the Union industry.

In its DSM mid-term review[40] of the progress made, published on 10 May 2017, the Commission outlined further actions on *online platforms, data economy and cybersecurity.*

In September 2017, as part of the State of the Union package, the Commission presented a proposal for new rules on the *free flow of non-personal data*[41] in the EU as well as a legislative proposal for a new and reinforced mandate for ENISA the *'European Cybersecurity Agency'* and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')[42]. Action in the field of cybersecurity is a priority. Indeed, whereas digital technologies open

[38] Regulation (EU) No 283/2014 of the European Parliament and of the Council of 11 March 2014 on guidelines for trans-European networks in the area of telecommunications infrastructure and repealing Decision No 1336/97/EC, OJ L 86, 21.3.2014, p. 14.

[39] Regulation (EU) 2017/1953 of the European Parliament and of the Council of 25 October 2017 amending Regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the promotion of internet connectivity in local communities, OJ L 286, 1.11.2017, p. 1.

[40] COM(2017) 228 final.

[41] COM(2017) 495 final.

[42] COM(2017) 477 final.

up new opportunities for citizens to connect, to exchange information and form the backbone of Europe's economy, they have also brought about new risks as evidenced by the worrying rise in cyberattacks.

The new measures on the *free flow of non-personal data,* together with the already existing rules for personal data, should enable the storage and processing of data across the Union to boost the competitiveness of European businesses and to modernise public services in an effective EU single market for data services. In the Council the proposal has been debate and agreement has been reached on 20 December 2017 at COREPER level on a text which should set the mandate for discussions with the European Parliament. In the European Parliament the file has been assigned to the Internal Market and Consumer Protection Committee.

2. The e-Commerce Directive (2000/31/EC)

The e-Commerce Directive, adopted in 2000, sets up an Internal Market framework for electronic commerce, which provides legal certainty for business and consumers alike. It has removed a series of obstacles to cross-border online services. The Directive is based on Article 114 TFEU, together with Articles 52 and 62 TFEU on establishment and on services, respectively. It is therefore clearly placed in the Single Market context. Its internal market clause, which states that the Member States may not restrict the freedom to provide information-society services from another Member State, is the cornerstone of the Digital Single Market.

2.1. Objectives and scope

The objectives of the Directive are set out in Article 1. Article 1(2) stipulates that the 'Directive approximates, to the extent necessary for the achievement of the objective set out in paragraph 1, certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States'. Paragraphs 3, 4 and 6 introduce limitations and paragraph 5 lists areas to which the Directive does not apply. According to paragraph 3, the Directive does not prejudice any protection of public health or consumers 'in so far as this does not restrict the freedom to provide information society services'; paragraph 4 states that the Directive does not establish additional rules on private international law nor does it deal with the jurisdiction of courts; paragraph 6 excludes measures taken in order to promote cultural and linguistic diversity and to ensure the defence of pluralism; paragraph 5 excludes certain areas from its scope (taxation, data protection, telecommunications, competition law applicable to cartels, notaries, lawyers and gambling).

2.2. Definitions

Article 2 contains the definitions for the purpose of the Directive. Central to the functioning of the Directive is the definition of information society services. The latter is not defined by the Directive itself but by reference to Article 1(2) of Directive 98/34/EC[43]. Recital 17 of the e-Commerce Directive states that 'this definition covers any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service; those services referred to in the indicative list in Annex V to Directive 98/34/EC which do not imply data processing and storage are not covered by this definition.' Recital 18 explains that information society services span a wide range of economic activities which take place on-line. Those activities go beyond on-line contracting and also 'extend, in so far as they represent an economic activity, to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service. They also include services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are information society services.'

The Court of Justice had very recently the opportunity to clarify in the *Uber* judgment[44] whether services provided by Uber (more specifically, its UberPop service), a platform that connects by means of a smartphone application passengers and non-professional drivers, qualifies as an information society service. The Court held in paragraph 35 of its judgment that:

> "... an intermediation service that enables the transfer, by means of a smartphone application, of information concerning the booking of a transport service between the passenger and the non-professional driver who will carry out the transportation using his or her own vehicle, meets, in principle, the criteria for classification as an 'information society service' within the meaning of Article 1(2) of Directive 98/34 and Article 2(a) of Directive 2000/31. That intermediation service, according to the definition laid down in Article 1(2) of Directive 98/34, is 'a service normally provided

[43] Directive 98/34/EC has been replaced by Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification), OJ L 241, 17.9.2015, p. 1.
[44] C-434/15, *Asociación Profesional Élite Taxi v Uber Systems Spain SL*, judgment of 20 December 2017, ECLI:EU:C:2017:981.

for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

The Court noted, however, 'that a service such as that in the main proceedings is more than an intermediation service consisting of connecting, by means of a smartphone application, a non-professional driver using his or her own vehicle with a person who wishes to make an urban journey' (paragraph 37). Indeed, Uber also organises the general operation of the intermediation service, including, the selection of non-professional drivers using their own vehicle 'to whom the company provides an application without which (i) those drivers would not be led to provide transport services and (ii) persons who wish to make an urban journey would not use the services provided by those drivers. In addition, Uber exercises decisive influence over the conditions under which that service is provided by those drivers.' (paragraph 39). The Court therefore concluded that the intermediation service provided by Uber 'must be regarded as forming an integral part of an overall service whose main component is a transport service and, accordingly, must be classified not as 'an information society service' within the meaning of Article 1(2) of Directive 98/34, to which Article 2(a) of Directive 2000/31 refers, but as 'a service in the field of transport' within the meaning of Article 2(2)(d) of Directive 2006/123' (paragraph 40).

This judgment is important in relation to Uber whose activities have given rise to great controversy and to conflicting judicial decisions in the various Member States.[45] Moreover, although the specificities of the case at hand appear to have shaped the judgment to a considerable extent, it also seems of relevance for other platforms active in the transportation sector and more generally for the so-called collaborative economy. Indeed, it seems to confirm the approach taken by the Commission in its Communication '*A European agenda for the collaborative economy*'[46] in which it considers that whether a collaborative platforms can be considered as offering other services in addition to the information society services that they offer to intermediate between the providers of underlying services and their users should be determined on a case-by-case basis, taking account in particular the level of control or influence that the platforms exert over the provision of the underlying services. This Communication provides guidance and policy orientation to public authorities, market operators and interested citizens on how existing EU law should be applied to the collaborative economy. The rules to which the Communication refers are those affecting the market access

[45] For examples of national court cases, see 'CARING FOR SHARING? THE COLLABORATIVE ECONOMY UNDER EU LAW' by Vassilis Hatzopoulos and Sofia Roma, Common Market Law Review 54: 81–128, 2017, section 2.

[46] COM(2016)356 final.

of the platforms and of the underlying services, their liability, consumer protection, labour law and taxation.

2.3. Main goals

The e-Commerce Directive has essentially three main goals. The *first goal* is to facilitate the establishment and operation of information society service providers within the internal market. To that effect, the Directive establishes two important principles: the 'country of origin', and the 'exclusion of prior authorisation'.

The 'country of origin' principle is laid down in Article 3(1), according to which 'each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field'[47],[48]. In simple terms, the 'country of origin principle' means that an information society service should be entitled to free movement if it is legal according to the law of the Member State where it originates. More concretely, this rule gives competence to the Member State where the service originates. Regarding the host Member States, Article 3(2) prevents restricting the freedom to provide information society services from another Member State for reasons falling within the coordinated field[49]. However, the host Member State may, pursuant to paragraph 4, derogate from the principle of the country of origin and be, therefore, allowed to impose its own measures if (i) the measure

[47] Recital 19 states that '[T]he place at which a service provider is established should be determined in conformity with the case-law of the Court of Justice according to which the concept of establishment involves the actual pursuit of an economic activity through a fixed establishment for an indefinite period; this requirement is also fulfilled where a company is constituted for a given period; the place of establishment of a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but the place where it pursues its economic activity; in cases where a provider has several places of establishment it is important to determine from which place of establishment the service concerned is provided; in cases where it is difficult to determine from which of several places of establishment a given service is provided, this is the place where the provider has the centre of his activities relating to this particular service.' In Case C-55/94 *Gebhard*, [1995] ECR 4165 EUCLI: EU:C:1995:411 the Court held that '[T]he concept of establishment within the meaning of the Treaty is a very broad one, allowing a Community national to participate, on a stable and continuous basis, in the economic life of a Member State other than his State of origin and to profit therefrom, so contributing to economic and social interpenetration within the Community in the sphere of activities as self-employed persons (see, to this effect, Case 2/74 *Reyners* v *Belgium* [1974] ECR 631, paragraph 21).

[48] Article 2 defines the 'coordinated field' as 'requirements laid down in Member States' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them'.

[49] According to paragraph 3, the two preceding paragraphs shall not apply to a number of areas listed in the Annex: Copyright and neighbouring rights, electronic money, choice of law, consumer contracts, real estate contracts and spam.

is necessary for one of the reasons indicated therein, (ii) taken against a given information society service which prejudices the objectives listed in point (i) or which presents a serious and grave risk to prejudice them, (iii) if the measure is proportionate to those objectives. In addition to these substantive conditions, the host Member State will also need to respect certain procedural requirements, including informing the Commission.

In its judgment of 25 October 2011, *eDate Advertising*[50], the Court of Justice clarified that Article 3 of the e-Commerce Directive precludes, subject to derogations authorised in accordance with the conditions set out in Article 3(4), a provider of an electronic commerce service from being made subject to stricter requirements than those provided for by the substantive law in force in the Member State in which that service provider is established.

The principle of 'exclusion of prior authorisation' is laid down in Article 4. Paragraph 1 provides that 'Member States shall ensure that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorisation or any other requirement having equivalent effect'. This rule is however without prejudice, in particular, to authorisation schemes which are not specifically and exclusively targeted at information society services (cf. Article 4(2)).

The *second goal* of the e-Commerce Directive is the provision of information by providers of information society services about themselves (Article 5) and in electronic commercial communications (Articles 6 to 8). In this regard, it is worth noting that the e-Commerce Directive applies in principle to both business-to-consumers[51] transactions and to business-to-business transactions.

The *third goal* is to create an exemption from liability for certain categories of intermediary service providers qualifying as a 'mere conduit' activity, a type of storage called 'caching' and a 'hosting' activity under Articles 12, 13 and 14 respectively[52]. This regime of liability exemption (also called 'safe harbour') extends to all kinds of legal responsibility issues, including criminal. For instance, even if the nature, characteristics and harm connected to terrorism-related material, illegal hate speech or child sexual abuse material or those related to trafficking in human beings are very different from violations of intellectual property rights, product safety rules, illegal commercial practices online, or online activities of a defamatory nature, all these different types of illegal content fall under the same overarching legal framework set by the e-Commerce Directive.

[50] Joined Cases C-509/09 and C-161/10, *eDate Advertising GmbH v X a.o.*, ECLI:EU:C:2011:685, at paragraph 67 (*eDate Advertising a.o.*).

[51] Several recitals refer to consumers (e.g. recitals 11, 30, 32, 53, 56) even if consumer protection is not the focus of the Directive.

[52] See also recitals 42 to 46.

Another important provision of the e-Commerce Directive is Article 15 which prevents Member States from imposing a general obligation on providers covered by Articles 12, 13 and 14 to monitor information which they transmit or store.

Liability issues and court injunctions (for which the safe harbour offers no protection) have led to a number of decisions of the Court of Justice giving it the opportunity to clarify important aspects of the regime established by the e-Commerce Directive, such as the identification of service providers that may benefit from the exemption, the criteria for the application of the exemption from liability and issues concerning jurisdiction in cases of publication of information on the internet adversely effecting personality rights, as further detailed below.

2.4. Liability regime for intermediary service providers

Information society service providers may benefit from the regime of liability exemption if, first, their activities qualify as 'information society services', within the meaning of Article 2(a) of the Directive and, second, if their activity entails the provision of 'mere conduit', 'caching' or 'hosting' services in the sense of Articles 12, 13 and 14 respectively.

Concerning the concept of 'information society services', case-law confirms that it covers only those services normally provided for remuneration. This means that those services must represent an economic activity. However, an 'information society service' within the meaning of Article 2(a) may be qualified as such even if its service is provided free of charge for the recipient of such service. Indeed, the remuneration does not need to be paid by those for whom the activity is performed[53]. For example, the service may be paid by advertising the goods sold and services provided by that service provider, since the cost of that activity is incorporated onto the price of those goods or services or by income generated by advertisements posted on a website[54].

In order to be able to benefit from the exemption from liability, the activity concerned must be: a) merely technical, automatic and passive so that the information society service provider does not have actual knowledge of the illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; b) in cases covered by Article 14, upon obtaining such knowledge or awareness, the service provider concerned shall act expeditiously to remove or to disable access to the information.

[53] C-484/14, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*, not yet reported, ECLI:EU:C:2016:689, at paragraphs 41and 42 (*Tobias Mc Fadden*).

[54] C-291/13, *Papasavvas v. O Fileleftheros Dimosia Etaireia Ltd a o.*; not yet reported, ECLI:EU:C:2014:2209, at paragraphs 28 and 29 (*Papasavvas*).

a) Technical, automatic and passive nature of the activity: this requirement, which applies to the activities covered by Articles 12(1), 13(1) and 14(1) respectively, implies that that service provider must play a neutral role in the sense that its conduct is merely technical, automatic and passive.

Regarding the 'mere conduit' activity, the Court of Justice confirmed that Article 12(1) must be interpreted as meaning that providing access to a communication network must not go beyond the boundaries of such a technical, automatic and passive process for the transmission of the required information. In order to benefit from the liability exemption, no further conditions need to be satisfied, such as a condition that there be a contractual relationship between the recipient and provider of that service or that the service provider use advertising to promote that service[55]. Furthermore, Article 12(1) does also not subject the exemption from liability to the condition that the provider must act expeditiously upon obtaining knowledge of illegal information to disable access to it[56].

The situation is different for 'hosting' services within the meaning of Article 14. Indeed, in order for the providers of such services to benefit from the exemption from liability laid down in that provision, in addition to the need of those services to be of mere technical, automatic and passive nature, pointing to a lack of knowledge or control of the data which they store, such providers upon obtaining knowledge of illegal information must act expeditiously to remove or to disable access to it[57].

More generally, if the provider of 'hosting' services, instead of confining itself to providing that service neutrally by a merely technical and automatic processing of the data provided by its customers, plays an active role of such a kind as to give it knowledge of, or control over, it may not benefit from the liability exemption. Whereas especially in relation to 'hosting' activities it may not always be easy to draw the line between passive and active behaviour of the service provider, several cases enabled the Court of Justice to clarify at least to some extent the situations in which a service provider can, or where the case may be, cannot benefit from the liability exemption. Indeed, in *Google France and Google*, the Court confirmed that the mere facts that a referencing service is subject to payment, that the operator of the search engine sets the payment terms or that it provides general information to its clients do not have the effect of depriving that operator of the exemptions from liability[58]. The same is valid for an online market place operator that stores offers for sale on its server, sets the terms of its

[55] *Tobias Mc Fadden*, at paragraphs 49 to 54.

[56] *Tobias Mc Fadden*, at paragraphs 57, 60 and 64.

[57] *Tobias Mc Fadden*, at paragraphs 58; C-236/08 to C-238/08, *Google France and Google*, ECR 2010 I-02417, ECLI:EU:C:2010:159, at paragraph 113 (*Google France and Google).*

[58] *Google France and Google*, at paragraph 116.

service, is remunerated for that service and provides general information to its customers, as confirmed in *L'Oréal v eBay*[59].

Conversely, the role played by an operator or a search engine in the drafting of the commercial message which accompanies the advertising link or in the establishment or selection of keywords may be relevant. Indeed, if it has played an active role of such a kind as to give it knowledge of, or control over, the data stored, it cannot benefit from the liability exemption[60]. The same is true when an online market place has provided assistance which entails optimising the presentation of the offers for sale or promoting those offers. In such a situation, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale[61]. Similarly, the Grand Chamber of the ECtHR held in *Delfi v Estonia*[62] that an operator of a news portal run on a commercial basis which published news articles of its own and invited its readers to comment on them and made those comments public, exercised a substantial degree of control over the comments published on its portal. The ECtHR confirmed that in that activity Delfi 'went beyond that of a passive, purely technical service provider'. It therefore, confirmed the findings by the domestic courts that the *Delfi* news portal was to be considered a provider of content services, rather than a provider of technical services, and that it should have effectively prevented clearly unlawful comments from being published. The fact that *Delfi* had immediately removed insulting content after having received notice of it did not suffice to exempt *Delfi* from liability.

b) Acting expeditiously after obtaining knowledge to remove or to disable access to the information: An information society service may obtain knowledge of illegal content hosted or conveyed by its services by different means, such as a notice by a user, by any other person or an injunction by a public authority, including a court.

It is worth recalling that Article 15(1) of the e-Commerce Directive prevents Member States from imposing a general obligation on intermediary service providers to monitor information which they transmit or store. That prohibition however only concerns obligations of a general nature and does not concern monitoring obligations in a specific case (see also recital 47).

The reasons for this general prohibition are to be found in Union primary law and, in particular, the Charter of Fundamental Rights (Charter). First, freedom of expression and information is protected under Article 11 of the Charter,

[59] C-324/09, *L'Oréal v eBay, ECLI:EU:C:2011:474*, at paragraph 115 (*L'Oréal v eBay*).

[60] *Google France and Google*, at paragraph 118 and 120.

[61] *L'Oréal v eBay*, at paragraph 113.

[62] European Court of Human Rights ('ECtHR'), *Delfi v. Estonia*, judgment of 16 June 2015, Application No 64569/09.

Article 10 ECHR and the Constitutions of Member States. Second, Article 7 of the Charter protects the fundamental right to privacy and communications and Article 8 thereof protects the right to personal data. Third, when such fundamental rights conflict with other fundamental rights and freedoms of others, e.g. in case of infringement of intellectual property rights enshrined in Article 17(2) of the Charter, a fair balance must be struck between the various fundamental rights protected by the Community legal order[63].

The Court confirmed in *Scarlet Extended*[64], that the prohibition of a general obligation on intermediary service providers (ISP) to monitor information applies in particular to national measures, and likewise their application by the national courts, which would require an ISP, such as an internet service provider, to actively monitor all the data of each of its customers in order to prevent any future infringement of intellectual-property rights[65]. Consequently, an injunction against an ISP requiring it to install a system for filtering all electronic communications passing via its services, which would apply indiscriminately to all its customers, as a preventive measure, which was capable of identifying on that provider's network the movement of electronic files (i.e. general monitoring) with a view to blocking the transfer of files the sharing of which would infringe copyright, is prohibited by Article 15(1) of Directive 2000/31[66]. Indeed, in adopting such an injunction, the national court concerned would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other[67].

2.5. llegal content: 'Notice and take-down'

At present there is no harmonised and coherent approach at Union level to remove illegal content online. Indeed, different approaches exist in the EU depending on Member States, content category, or type of online platform. The e-Commerce Directive does not lay down procedural rules to that effect and privileges the drawing up of codes of conduct at Union level *designed to contribute to the proper implementation of Articles 5 to 15*.[68]

[63] C-275/06, *Promusicae* [2008] ECR I-271, ECLI:EU:C:2008:54, at paragraph 68.
[64] Case C-70/10 *Scarlet Extended*, ECLI:EU:C:2011:771, at paragraph 36 (*Scarlet Extended*).
[65] *Scarlet Extended*, at paragraph. 37.
[66] *Scarlet Extended*, at paragraph 40. See also C-360/10, *SABAM v Netlog NV*, ECLI:EU:C:2012:85, at paragraph 38 (*SABAM v Netlog*).
[67] *Scarlet Extended*, at paragraph 53. See also *SABAM v Netlog*, at paragraphs 45 to 51.
[68] Cf. Article 16 and recital 49.

However, the issue of taking down or disabling access to illegal content online and the procedures to be followed to that effect have become acute, essentially for two main reasons.

The first reason is linked with the generalised use of online platforms. Today most people get access to information on the internet through search engines, social networks, blog sites, or video-sharing platforms. Those platforms connect billions of users with vast quantities of content and information, generated either by the platforms and/or by the users. Their business models rely more and more on the establishment of a link between users and content, in particular for targeted advertising. However, content accessible online may be illegal under Union or national law. Such may be the case, e.g. of content on incitement to terrorism, xenophobic and racist speech that publicly incites hatred and violence or child sexual abuse material. Other types of content, while not illegal in nature, may harm trust because of their intentional inaccurate or false information ('fake content'), sometimes used as part of disinformation campaigns designed to influence users' choices, including policy choices.

The second reason is related to individual rights, such as the right to intellectual property, rights to reputation of natural or legal persons and the rights to privacy and to the protection of personal data. Regarding the latter, following the *Google Spain*[69] ruling of the Court of Justice, the question of delisting information from results of search engines gave rise to a lively debate between those who see a danger to information rights and to the internet as an open platform for democratic participation and those who see a need to prevent unjustified interferences with privacy rights. Blocking, filtering and taking-down content from the internet raises delicate legal issues as regards the balance to be stricken between certain public interests and various fundamental rights, such as freedom of expression and information, recognised under Article 10 ECHR and 11 of the Charter, the protection of personal data under Article 8 of the Charter and the fundamental right to property under Article 17 thereof, which includes the rights linked to intellectual property, as well as the freedom to conduct a business enjoyed by operators such as ISPs pursuant to Article 16 of the Charter.

According to a comparative study of the Council of Europe (CoE), published in 2017[70], there are essentially two general categories of national regulatory 'models':

On the one hand, there are countries which do not have any specific legislation on the issue of blocking, filtering and takedown of illegal internet content. Several countries, such as Germany, Austria, the Netherlands, the United

[69] C-131/12, *Google Spain SL v Agence Española de Protección de Datos*, EUCI:EU:C:2014:317 (*Google Spain*).
[70] https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html

Kingdom, Ireland, Poland, the Czech Republic and Switzerland, rely on an existing "general" legal framework that is not specific to the internet to conduct limited blocking or takedown of unlawful online material. On the other hand, there are countries in which the legislator has intervened in order to set up a legal framework specifically aimed at regulating the internet and other digital media, including the blocking, filtering and removal of internet content. Such legislation typically provides for the legal grounds on which blocking or removal may be warranted, the administrative or judicial authority which has competence to take appropriate action and the procedures to be followed.

Under Union law, certain categories of content are considered illegal and must be removed swiftly from the internet or access must be blocked or disabled.

A first example of illegal content is any 'conduct publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin' as provided for in Article 1(a) of the Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law[71].

A second example is child abuse material under Directive (EU) 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography[72] (Child Pornography Directive). Article 25 of this Directive has the main objective of disrupting the availability of child pornography online. It provides that Member States are obliged to (i) remove promptly material on websites hosted within their territory; (ii) endeavour to secure the removal of material on websites hosted elsewhere; and (iii) to offer the possibility to block access to child pornography by users within their territory[73].

A third example is in Directive (EU) 2017/541 of 15 March 2017 on combating terrorism[74] (Terrorism Directive). Pursuant to Article 21 of this Directive, Member States are required to take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence. If removal of illegal content at its source is not feasible, Member States may take measures to block access to such content towards the internet users within their territory.

Both the Child Pornography Directive and the Terrorism Directive require the measures for removal and blocking to be set following transparent

[71] Cited under footnote 22.

[72] OJ L 335, 17.12.2011, p. 1.

[73] For more information, see report of the Commission on the implementation of Article 25 of Directive 2011/93/EU (COM(2016) 872 final).

[74] Directive (EU) 2017/541 of 15 March 2017 on combating terrorism and replacing Council framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88 of 31.3.2017, p. 6.

procedures and to provide for adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. They furthermore provide that those safeguards are to include the possibility of judicial redress.

The abovementioned CoE study states that in relation to child abuse material, terrorism, criminality (in particular hate crimes) and national security, many of the States that with targeted legal rules for the removal of internet content provide for the urgent blocking of such material without the need for a court order. Administrative authorities, police authorities or public prosecutors are given specific powers to order internet access providers to block access without prior judicial authority. An internet access provider is required to take action, in general, within 24 hours and without any notice being given to the content provider or host themselves. In other countries where a court order is otherwise needed, hosting providers who have knowledge of such material may be expected to remove it voluntarily without judicial authority and to provide the content provider with due notice, which permits them to challenge the action through the courts.

Concerning content covered by the Child Pornography Directive hosted in the Union[75], Member States have adopted two types of measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory. Those are measures based on e-Commerce Directive and measures based on national criminal law[76]. Regarding the former, a service provider that hosts content can benefit from the liability exemption if the conditions provided for under Article 14 of that Directive are fulfilled, i.e. that the ISP has neither knowledge of nor control over the information that is transmitted or stored, and upon obtaining actual knowledge or awareness of illegal activities, it acts expeditiously to remove or to disable access to the information concerned. The procedures for notice and take down take the form of mechanisms run by interested parties aimed at identifying illegal information hosted on the network and at facilitating its rapid removal. Member States have implemented notice and take down procedures through national hotlines, to which internet users can report child sexual abuse material that they find online[77]. INHOPE is the umbrella organisation for the hotlines.

[75] For more information on the content hosted outside a Member State's territory, see section 2.1.1. of the Commission's report on the implementation of Article 25 of Directive 2011/93/EU, cited under footnote 75.

[76] For the types of measures implemented by the MS, see p. 8 of the Commission's report on the implementation of Article 25 of Directive 2011/93/EU, cited under footnote 75.

[77] Such as information society service providers (ISSPs), including providers of access, hosting and online platforms, internet users, who may come across child sexual abuse material online (intentionally

As indicated above, there are no procedural rules at Union level for notice and taking down illegal content and the e-Commerce Directive privileges the drawing up of codes of conduct. In order to steer and promote further self-regulatory action, the Commission has set up a number of sectoral dialogues with stakeholders and initiated other self-regulatory mechanisms.

One such Code of Conduct was signed by the Commission on 31 May 2016[78] with four main tech companies (Facebook, Microsoft, Twitter and YouTube) active in the area of social networking and hosting online content on the delicate issue of countering illegal hate speech online. The platforms concerned committed to use it for guiding their own activities and sharing best practices with other internet companies, platforms and social media operators. They also commit, *inter alia*, to have in place clear and effective processes to review notifications regarding illegal hate speech on their services; to have in place rules or guidelines clarifying that they prohibit the promotion of incitement to violence and hateful conduct; having dedicated teams reviewing requests and, fallowing valid notifications, remove illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary.

This action was fostered by the particular factual context of the terrorist attacks in Paris in 2015 and in Brussels in March 2016. The political impulse was given by the EU Ministers for Justice and Home Affairs and representatives of EU institutions in a Joint Statement issued on 24 March 2016 on the terrorist attacks in Brussels on 22 March 2016[79]. It indicates that the *Commission will intensify work with IT companies, notably in the EU Internet Forum, to counter terrorist propaganda and to develop by June 2016 a code of conduct against hate speech online*.

More generally, considering that access to information and content platforms are increasingly taking centre stage, the Commission adopted two Communications on platforms, the first on 25 May 2016[80] and the second on 28 September 2017[81]. Whereas the first Communication has two main objectives, namely, to outline

or unintentionally) and decide to report it to the ISSP directly if the technology to do so is in place, e.g. through a 'report abuse' button on the web page or browser, dedicated hotlines, usually run by an NGO or an association of ISSPs or media companies, which allow anonymous reporting by users who may not feel comfortable reporting to the police and cannot or do not wish to report to the ISSP directly. See Commission's report on the implementation of Article 25 of Directive 2011/93/EU, cited under footnote 75.

[78] http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf

[79] Joint statement of EU Ministers for Justice and Home Affairs and representatives of EU institutions on the terrorist attacks in Brussels on 22 March 2016, available at: http://www.consilium.europa.eu/en/press/press-releases/2016/03/24-statement-on-terrorist-attacks-in-brussels-on-22-march/

[80] COM(2016) 288 final, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe.

[81] COM(2017) 555 final, Tackling Illegal Content Online Towards an enhanced responsibility of online platforms.

the key issues identified by the Commission in its assessment of online platforms and to present the Commission's position on both the innovation opportunities and the regulatory challenges presented by online platforms, and to set out its approach to supporting their further development in Europe, it nevertheless highlights the responsibility of platforms with regard to content and access to information. The second Communication addresses specifically the issue of tackling illegal content online. It recalls that the identification of what constitutes 'illegal' content must be determined by specific legislation at the EU level, as well as by national law. At EU level, the general legal framework laid down by the e-Commerce Directive, under which certain online platforms can benefit from the exemption from liability for illegal content which they host across the Digital Single Market, is applicable the for the removal of any illegal content. Given the significant similarities in the removal process for the different content types, the Communication covers the whole range of illegal content online, while allowing for sector-specific differences where appropriate and justified. It contains a set of (non-legally binding) guidelines and principles for online platforms to step up the fight against illegal content online in cooperation with national authorities, Member States and other relevant stakeholders in view of facilitating and intensifying the implementation of good practices for preventing, detecting, removing and disabling access to illegal content. It also seeks to address concerns in relation to removal of legal content, sometimes called 'over-removal', which in turn impacts freedom of expression and media pluralism. And, finally, it aims to provide clarifications to platforms on their liability when they take proactive steps to detect, remove or disable access to illegal content.

The Commission is now in the process of designing a monitoring strategy based on a combination of quantitative and qualitative indicators stemming from the actions identified in the Communication, as well as on dedicated dialogues with the industry and other stakeholders. The outcomes of its monitoring activities and further assessments and consultations will help it to determine whether additional measures are necessary and if so, which ones.

2.6. Jurisdiction in disputes concerning publication of information affecting personality rights

From the outset it is recalled that the e-Commerce Directive does not establish additional rules on private international law nor does it deal with jurisdiction of Courts, as provided for in Article 1(4).

Jurisdiction rules for civil and commercial matters in the European Union are laid down in Regulation (EU) N° 1215/2012[82] which replaced Regulation (EC) N°

[82] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 351, 20.12.2012, p. 1.

44/2001[83] (Brussels I Regulation). Article 7(2) of Regulation N.° 1215/2012 – identical to the wording of Article 5(3) of Brussels I Regulation – which forms part of Section 2, headed 'Special jurisdiction', provides that '[a] person domiciled in a Member State may be sued in another Member State [...] in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur.'

Settled case-law of the Court of Justice confirms, that that rule of special jurisdiction is based on the existence of a particularly close connecting factor between the dispute and the courts of the place where the harmful event occurred or may occur, which justifies the attribution of jurisdiction to those courts for reasons relating to the sound administration of justice and the efficacious conduct of proceedings[84]. It also confirms that the expression 'place where the harmful event occurred or may occur' is intended to cover both the place where the damage occurred and the place of the event giving rise to it, since each of them could, depending on the circumstances, be particularly helpful in relation to the evidence and the conduct of the proceedings[85].

In 1995 in *Shevill a.o.*[86], a case that concerned an action seeking compensation for non-material damage allegedly caused by a defamatory article published in the printed press, the Court has held that the victim may bring an action for damages against the publisher before the courts of each Member State in which the publication was distributed and where the victim claims to have suffered injury to his reputation. Such courts have jurisdiction to rule solely in respect of the harm caused in the Member State of the court seised.

In 2011, in the specific context of the internet, the Court has ruled in *eDate Advertising a.o.*[87] a case relating to a natural person, that, in the event of an alleged infringement of personality rights by means of content placed online on a website, the person who considers that his rights have been infringed must have the option of bringing an action for damages, in respect of all the harm caused, before the courts of the Member State in which the centre of his interests is based. Regarding the identification of the centre of interests, the Court has held that this generally corresponds to the Member State of his habitual residence. However, such a person may also have his centre of interests in a Member State in which he does not habitually reside, in so far as other factors, such as the

[83] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 12, 16.1.2001, p. 1

[84] See, inter alia, *eDate Advertising a.o.*, paragraph 40, and judgment of 22 January 2015, *Hejduk*, C-441/13, EU:C:2015:28, at paragraph 19 and the case-law cited.

[85] *eDate Advertising a.o.*, at paragraph 41 and the case-law cited.

[86] C-68/93, *Shevill a.o,* 7 March 1995, EU:C:1995:61, at paragraph 33.

[87] *eDate Advertising a.o.*, at paragraph 52.

pursuit of a professional activity, may establish the existence of a particularly close link with that State[88].

More recently, the Court interpreted the concept of 'centre of interest' of a legal person pursuing an economic activity in a case concerning the publication of information (and related comments) on a website. Indeed, in its judgement of 17 October 2017[89], the Court held that:

> '41. As regards a legal person pursuing an economic activity, such as the applicant in the main proceedings, the centre of interests of such a person must reflect the place where its commercial reputation is most firmly established and must, therefore, be determined by reference to the place where it carries out the main part of its economic activities. While the centre of interests of a legal person may coincide with the place of its registered office when it carries out all or the main part of its activities in the Member State in which that office is situated and the reputation that it enjoys there is consequently greater than in any other Member State, the location of that office is, not, however, in itself, a conclusive criterion for the purposes of such an analysis.'

It is worth noting that the Court replied in the negative to the first question put forward by the referring court asking whether Article 7(2) of Regulation N° 1215/2012 must be interpreted as meaning that a person who alleges that his personality rights have been infringed by the publication of incorrect information concerning him on the internet before the courts of each Member State in which the information published on the internet is or was accessible. In this regard, the Court replied as follows:

> '47. It is true that, in paragraphs 51 and 52 of the judgment of 25 October 2011, *eDate Advertising and Others* (C-509/09 and C-161/10, EU:C:2011:685), the Court held that the person who considers that his rights have been infringed may also, instead of an action for damages in respect of all the harm caused, bring his action before the courts of each Member State in whose territory content placed online is or has been accessible, which have jurisdiction only in respect of the harm caused in the territory of the Member State of the court seised.
>
> 48. However, in the light of the ubiquitous nature of the information and content placed online on a website and the fact that the scope of their distribution is, in principle, universal (see, to that effect, judgment of 25 October 2011, *eDate Advertising and Others*, C-509/09 and C-161/10, EU:C:2011:685, paragraph 46), an application for the rectification of the former and the removal of the latter is a single and indivisible application and can, consequently, only be made before a court with jurisdiction to

[88] *eDate Advertising a.o.*, at paragraph 49.

[89] C-194/16 *Bolagsupplsningen OÜ, a.o. v Svensk Handel AB*, ECLI:EU:C:2017:766.

rule on the entirety of an application for compensation for damage pursuant to the case-law resulting from the judgments of 7 March 1995, *Shevill and Others* (C-68/93, EU:C:1995:61, paragraphs 25, 26 and 32), and of 25 October 2011, *eDate Advertising and Others* (C-509/09 and C-161/10, EU:C:2011:685, paragraphs 42 and 48), and not before a court that does not have jurisdiction to do so.

49. In the light of the above, the answer to the first question is that Article 7(2) of Regulation No 1215/2012 must be interpreted as meaning that a person who alleges that his personality rights have been infringed by the publication of incorrect information concerning him on the internet and by the failure to remove comments relating to him cannot bring an action for rectification of that information and removal of those comments before the courts of each Member State in which the information published on the internet is or was accessible.'

3. Protection of Privacy and Personal Data

3.1. Primary law and Union legislative framework

The right to the protection of personal data is enshrined in Article 8 of the Charter as a distinct right, albeit closely linked to Article 7 of the Charter which enshrines the right to respect for private and family life, home and communications.

Articles 7 and 8 of the Charter read as follows:

Article 7 respect for private and family life

'Everyone has the right to respect for his or her private and family life, home and communications.'

Article 8 Protection of Personal Data

'1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.'

Article 52(1) of the Charter provides that:

'1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.'

Before the entry into force of the Lisbon Treaty, the Union acts on the protection of personal data were adopted on the basis of Article 95 TEC (now Article 114 TFEU) as no explicit legal basis for the adoption of rules on the protection of personal data existed in the former first pillar area. Directives 95/46/EC (Directive 95/46) on the protection of personal data, 2002/58/EC[90] on privacy and electronic communications (Directive 2002/58 or ePrivacy Directive) where based on Article 95 TEC[91]. The internal market legal basis is reflected in the objectives of these legal acts, namely to protect the right to privacy with respect to the processing of personal data as well as the free movement of personal data. Article 286 TCE, inserted by the Amsterdam Treaty, declared all existing Community Acts applicable to the Community institutions and bodies. Despite this declaration, a specific Regulation (45/2001[92]) containing data protection rules for such institutions and bodies was adopted. Its rules correspond, broadly, to the provisions of Directive 95/46. This Regulation also established an independent supervisory authority responsible for monitoring the application of the rules by the Community, the European Data Protection Supervisor (EDPS), as required by the second paragraph of Article 286 TEC.

With the entry into force of the Lisbon Treaty the Charter became legally binding and the right to the protection of personal data was also explicitly recognised in the Treaties. This right can be found in Article 16 TFEU and is also referred to in Article 39 TEU.

Article 16 TFEU grants everyone the right to the protection of personal data concerning them. It constitutes the new, self-standing legal basis for Union rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. This provision constitutes, without prejudice to Article 39 TEU, the appropriate legal basis for the adoption of an act by the Union legislature, where the protection of personal data is one of the essential aims or components, including in the area of judicial

[90] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.

[91] Directive 2006/24/EC on the retention of communications data was also based on Article 95 TEC. It was declared invalid by the Court in its judgment of 8 April 2014, Joined Cases C-293/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* and C-594/12 *Kärntner Landesregierung, Seitlinger and Others*, judgment of 8 April 2014, ECLI:EU:C:2014:238, not yet reported (*Digital Rights Ireland*).

[92] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1.

cooperation in criminal matters and police cooperation[93]. Both, the GDPR and the 'Police Directive'[94] are based on Article 16 TFEU.

3.2. The General Framework: the GDPR

Like its predecessor, the GDPR lays down a general framework for the protection of personal data. It incorporates the objectives and principles of Directive 95/46 which remain sound, therefore ensuring continuity of the existing framework in many respects. It introduces however, a quite important number of new elements aimed essentially at:

- enhancing data protection rights of individuals;
- making organisations more accountable;
- increasing the effectiveness of supervision and enforcement by Data Protection Authorities (DPAs)

Given the important number of changes introduced by the GDPR as compared with Directive 95/46, we will focus only on a selection of new elements.

To start with, there is the chosen *form* of the new act, a Regulation instead of a Directive. The reasons for this choice are explicit, in particular, in recitals 9 and 13. Indeed, recital 9 states that the differences in implementation of Directive 95/46 by Member States resulted in differences in the level of protection of the right to the protection of personal data and those differences may prevent the free flow of personal data throughout the Union. They may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Recital 13 explains that in order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing.

[93] Opinion of the Court of Justice of 26 July 2017, A-1/15 on the Draft agreement between Canada and the European Union on the transfer of *PNR* data, ECLI:EU:C:2017:592, at paragraph 96.

[94] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89.

Second, the *territorial scope* has been broadened (Article 3(2)) so that it also applies to controllers or processors not established in the Union, where the processing activities are related to the offering of goods or services to data subjects in the Union or, the monitoring of their behaviour. Such controllers must designate a representative in the Union pursuant to Article 27.

Third, the GDPR has enhanced the *data protection rights of data subjects*. Notably, the conditions for a valid consent as a ground for processing were reinforced. According to Article 4(11) consent means 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. Article 7 further specifies, inter alia, that consent may be withdrawn at any time. Recital 42 further states that 'consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment'. Furthermore, specific conditions have been added regarding child's consent in relation to information society services, as provided for under Article 8.

The right 'right to be forgotten' is explicit in Article 17. It will apply in certain specific cases listed in Article 17(1), such as where the data are no longer necessary in relation to the purposes for which they were collected or if the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing. That right is particularly relevant where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child[95]. Article 17(3) refers to cases in which it will be necessary to perform a balancing exercise between the right to be forgotten with other rights, such as the right of freedom of expression and information or the establishment, exercise or defence of legal claims or other important public interests.

A new right, the right to 'data portability' has been created (Article 20). This will give individuals the power to choose which service provider (e.g. social network, internet service provider) may handle their personal data. And they will be able to transfer all their data, in a structured, commonly used and machine-readable format to another higher quality competitor if they wish (e.g. because more privacy-friendly). This right may be exercised only in cases where processing is based on consent or on a contract and the processing is carried out by automated means.

[95] See recital 65.

Also, the GDPR specifically addresses profiling. Profiling is perhaps the concept that responds most directly to the challenges of Big Data. As the EDPS stated in its Strategy 2015-2019[96]:

'Big data that deals with large volumes of personal information implies greater accountability towards the individuals whose data are being processed. People want to understand how algorithms can create correlations and assumptions about them, and how their combined personal information can turn into intrusive predictions about their behaviour.'

Forth, the GDPR introduces two important changes regarding administrative and judicial remedies for data subjects:

(i) According to Article 79(2), the data subject can chose either to bring proceedings against a controller or processor in the courts of the Member State where the controller or processor has an establishment or, alternatively, before the courts of the Member State of his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers[97].

(ii) Article 80(1) allows a data subject to be represented by a not-for-profit body, organisation or association, which [...], has statutory objectives which are in the public interest, and is active in the field of data protection to lodge complaints and to exercise the rights to a judicial remedy against a supervisory authority, a controller or processor, including the right to receive compensation, on his or her behalf.

Fifth, the GDPR represents a paradigm shift insofar as undertakings are concerned. The previous system of prior notification of processing activities to supervisory authorities has been replaced by a system of 'comply and demonstrate'. Indeed, the GDPR imposes on controllers and processors the obligation to implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that processing is performed in accordance with the Regulation (Article 24). To that effect, organisations must, *inter alia*, maintain records of processing activities (Article 30), apply the principles of data protection by design and by default (Article 25), ensure the security of the data processing (Article 32) and, under certain conditions, to give notice of data breaches

[96] https://edps.europa.eu/sites/edp/files/publication/15-07-30_strategy_2015_2019_update_en.pdf

[97] Recital 147 States: 'Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) N° 1215/2012 of the European Parliament and of the Council should not prejudice the application of such specific rules.'

(Article 33), and perform data protection impact assessments (Articles 35 and 36) and designate a data protection officer (Article 37).

The obligations on controllers and processors are supported by strong incentives that may take the form of administrative fines, as provided for under Article 83[98], or penalties to be laid down by Member States pursuant to Article 84. Depending on the cases, administrative fines may be up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Finally, the GDPR enhances coordination of supervision of the implementation of the Regulation.

An important novelty is the so-called 'one-stop-shop mechanism'. Where a company has branches in more than one Member State, there will be one single supervisory authority – the "lead" supervisory authority. It will be the supervisory authority in the Member State of the company's main establishment in the Union (Article 56) that will have the competence for supervising compliance with the Regulation. Pursuant to Article 60 the lead supervisory authority shall cooperate with the other supervisory authorities concerned.

Furthermore, the current Article 29 Working Party will be replaced by the European Data Protection Board (EDPB), a new Union body, having its own legal personality and consisting of the national supervisory authorities and the European Data Protection Supervisor. The EDPB will have its own powers to take decisions, adopt opinions and guidelines, (as provided for under Article 70). Importantly, pursuant to Article 65(1), the Board will act as a dispute resolution body and have the power to adopt a binding decision in the following cases:

a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

[98] Paragraph (7): Member States may lay down the rules as to whether and to what extent administrative fines may be imposed on public authorities and bodies.

3.3. The Union rules on ePrivacy

3.3.1. Current rules

The ePrivacy Directive (2002/58) specifically governs the processing of personal data by providers of electronic communications services falling within its scope. It therefore must be regarded as a lex specialis[99], as is explicit in Article 1(2) thereof.

For a correct understanding of the relationship between the GDPR and the ePrivacy Directive, it is useful to recall that both acts have as their main purpose to implement to different degrees Articles 7 and 8 of the Charter. Indeed, the GDPR constitutes a detailed elaboration of Article 8 whereas the ePrivacy Directive implements Articles 7 and 8. It should be noted that the ePrivacy Directive is so far the only instrument in Union secondary law that comprehensively implements the principle of confidentiality of communications enshrined in Article 7 of the Charter, by laying down rules on the processing of traffic, communication and location data and the protection of terminal equipment. Vis-à-vis the GDPR it particularises data protection rules for the specific economic sector to which it applies. The ePrivacy Directive also ensures the confidentiality of communications of legal persons and protects their legitimate interests in this regard.

The need to protect confidentiality of communications has long been recognised. It is part of Article 8 ECHR[100] as interpreted by the ECtHR[101] and is in line with the constitutional traditions of EU Member States. Indeed, the majority of EU Member States recognise confidentiality of communications as a distinct constitutional right[102]. At EU level, Directive 97/66/EC[103] was the first specific Directive for the processing of personal data in the telecommunications sector, the predecessor of the ePrivacy Directive. The obligation to protect the confidentiality of traditional correspondence has been integrated in EU law

[99] This is also explicit in Recital 173: it states that the GDPR applies to all matters concerning the processing of personal data which are not subject to specific obligations with the same objective set out in the ePrivacy Directive, including the obligations on the controller and the rights of natural persons.

[100] Article 8(1) ECHR: 'Everyone has the right to respect for his or her private and family life, home and correspondence.'

[101] See most recently *Bărbulescu v. Romania* [GC], Application no. 61496/08, judgment of 5 September 2017 at paras. 72-73. All ECtHR decisions are available online at http://hudoc.echr.coe.int/.

[102] The EDPS Preliminary Opinion 5/2016 on the review of the ePrivacy Directive, in footnote 11 lists the following examples: Article 10 of the German Constitution, Article 37 of the Slovenian Constitution, Article 36 of the Croatian Constitution, Article 19 of the Greek Constitution, Article 43 of the Estonian Constitution, Article 15 of the Italian Constitution, Article 49 of the Polish Constitution, Article 28 of the Romanian Constitution, Article 72 of the Danish Constitution, Article 13 of the Dutch Constitution, Article 29 of the Belgian Constitution, Article 6 of Chapter 2 of the Swedish Constitution, Article 10 of the Finnish Constitution, Article 17 of the Cypriot Constitution, Article 18 of the Spanish Constitution, Articles 10 and 10a of the Austrian Constitution, Article 13 of the Czech Constitution and Article 22 of the Slovak Constitution.

[103] OJ L 24, 30.1.1998, p. 1.

with the adoption of Directive 97/67/EC on postal services[104] (cf. Article 2(19)). It should be noted that rules on the protection of communications apply to both natural and legal persons. The inclusion of legal persons in the scope of these rules is connected with the scope of Article 7 of the Charter which contains rights corresponding to those guaranteed by Article 8(1) of the ECHR. In accordance with Article 52(3) of the Charter, Article 7 thereof is thus to be given the same meaning and the same scope as Article 8(1) of the ECHR, as interpreted by the case-law of the ECtHR[105]. Concerning the scope of Article 7 as concerns legal persons, the case-law of both the Court of Justice[106] and of the ECtHR[107] confirms that professional activities of legal persons may not be excluded from the protection of the right guaranteed by both Article 7 of the Charter and Article 8 of the ECHR.

3.3.2. The proposal for the ePrivacy Regulation

Recital 173 the GDPR states that once this Regulation is adopted the ePrivacy Directive should be reviewed, in particular to ensure consistency with this Regulation. In reply to this call by the co-legislators, the Commission adopted the proposal for the ePrivacy Regulation on 10 January 2017[108]. The text of Article 1(3) of that proposal is similar to current Article 1(2) and provides that the provisions of the ePrivacy Regulation 'particularise and complement' the GDPR 'by laying down specific rules [...]'.

The Commission's choice of the instrument (a Regulation) follows the same rationale as for the GDPR: to ensure legal certainty for users and businesses alike by avoiding divergent interpretation and implementation in the Member States. It is also justified for reasons of consistency with the GDPR.

The proposal contains a set of targeted measures aimed at ensuring effective protection of the fundamental right to privacy and communications. To that effect, it lays down the principle of confidentiality of communications and

[104] Directive 97/67/EC of the European Parliament and of the Council of 15 December 2007 on common rules for the development of the internal market for Community postal services and the improvement of quality of service, OJ L 15, 21.1.2008, p. 14.

[105] Case C-419/14, *WebMind Licenses Kft.*, judgment of 17 December 2015, not yet reported (ECLI:EU:C:2015:832), at paragraph 70 and case-law cited therein.

[106] C-450/06, *Varec SA v Belgian State*, [2008] I-581 (ECLI:EU:C:2008:91), at paragraph 48.

[107] See, inter alia, ECtHR judgments *Niemietz v Germany*, judgment of 16 December 1992, Series A n° 251-B, §29; *Société Colas Est and Others v France*, no 37971/97, at paragraph 41; ECHR 2002-III; *Peck v The United Kingdom* n° 44647/98, at paragraph 57, ECtHR 2003-I; and also *Vinci Construction and GTM Génie Civil et Services v. France*, n°s. 63629/10 and 60567/10, at paragraph 63, 2 April 2015.

[108] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), (COM(2017) 10 final).

identifies exhaustively the permitted processing of communications data. It enlarges the personal scope of the current ePrivacy Directive to extend to Over-the-Top communications services ("OTTs")[109]. This takes into account the reality that users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services.

The proposal also extends the principle of confidentiality of communications to the transmission of machine-to-machine communications and reinforces the protection of privacy of terminal equipment[110]. The alignment with the GDPR resulted in incorporating its definitions, territorial scope and the supervision and consistency mechanism into the proposal for ePrivacy Regulation. It also resulted in the omission in the proposal of some provisions, such as the security and data breach notification obligations of current Article 4 of the ePrivacy Directive, to ensure that those provisions already in the GDPR will apply. Finally, as the rules on ePrivacy apply also to legal persons, certain provisions of the GDPR will be applicable to these category of end-users, notably those on consent and on legal remedies and compensation, as provided for under Articles 77, 78, and 79 as well as Article 82 GDPR.

The European Parliament decided on 23 October 2017 that the LIBE report[111], containing 168 amendments, constitutes the basis for negotiations with the Council at first reading[112]. In the Council the proposal continues being discussed the level of the Working Party. At the time of writing, it is unlikely that the proposal will be adopted on time for entering into application on the same date as the GDPR, i.e. 25 May 2018 as proposed by the Commission.

[109] The ePrivacy Directive is part of the regulatory framework for electronic communications. This framework was revised in 2016 following which the Commission adopted the proposal for a Directive establishing the European Electronic Communications Code ("EECC") (COM/2016/0590 final). The proposal for ePrivacy Regulation, partially relies on definitions provided in the EECC, including that of 'electronic communications services'. Like the EECC, the ePR proposal also brings OTTs in its scope to reflect the market reality.

[110] The Explanatory Memorandum accompanying the proposal states that 'the consent rule to protect the confidentiality of terminal equipment failed to reach its objectives as end-users face requests to accept tracking cookies without understanding their meaning and, in some cases, are even exposed to cookies being set without their consent. The consent rule is over-inclusive, as it also covers non-privacy intrusive practices, and under-inclusive, as it does not clearly cover some tracking techniques (e.g. device fingerprinting) which may not entail access/storage in the device. Finally, its implementation can be costly for businesses'.

[111] Ref. A8-0324/2017, available at:, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0324&language=EN

[112] http://www.europarl.europa.eu/sides/getDoc.do?type=PV&reference=20171026&secondRef=ITEM-010-05&language=EN&ring=A8-2017-0324

3.4. Specific legislative Union acts may contain specific provisions on the processing of personal data

The GDPR lays down a general framework for the protection of personal data in the Union. Other Union acts (in other fields than police cooperation, criminal law and Union institutions, bodies, offices and agencies) may clarify that they apply without prejudice to the GDPR. If the data subject's rights (e.g. to information, access, rectification, erasure, restriction, portability, etc.) are not intended to be restricted by the Union specific legislative act, there is no need to reproduce them in that act, since the GDPR will apply.

Where processing is necessary for compliance with a legal obligation (Article 6(1)(c)) or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e)), the basis for processing shall be laid down by Union or Member State law as required by Article 6(3) of the GDPR. This provision indicates what the basis for data processing shall and may specify: the purpose of the processing shall be determined in the legal basis which may contain specific provisions to adapt the application of rules of this Regulation (e.g. the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which the personal data may be disclosed; the purpose limitation, storage periods, ...). Article 6(3) further requires that such law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

3.5. Brief summary of selected case-law of the Court of Justice

The Court of Justice has on several occasions ruled on the interpretation of the Data Protection Directive, the ePrivacy Directive and other Union acts containing provisions on the processing of personal data. The Court has consistently held that that derogations and limitations in relation to the protection of the fundamental rights enshrined in Articles 7 and 8 of the Charter must apply only in so far as is *strictly necessary*.

Concerning publication of personal data, in its *Schecke*[113] judgement of 9 November 2010, the Court examined the validity of provisions of Union law laid down in two Regulations providing for the publication of information on beneficiaries of EAGF and EAFRD aid. The Court concluded that the concerned provisions were invalid in so far as, with regard to natural persons who were beneficiaries of EAGF and EAFRD aid, those provisions imposed an obligation to publish personal data relating to each beneficiary without drawing a distinction based on relevant criteria such as the periods during which those persons have received such aid, the frequency of such aid or the nature and amount thereof.

[113] Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR* and *Hartmut Eifert*, ECLI:EU:C:2010:662, at paragraph 86.

Concerning the processing of personal data and privacy in the electronic communications sector, in particular, data retention, the Court focused on the relevant provisions of the ePrivacy Directive. Such was the case in its landmark judgments *Digital Rights Ireland* and *Tele2 Sverige and Watson*[114] both concerning the compatibility of data retention measures (EU and national, respectively) with the Charter.

In *Digital Rights Ireland* the Court declared Directive 2006/24/EC invalid, leaving national data protection measures under the aegis of the derogation in Article 15 of the ePrivacy Directive.

In *Tele2 Sverige and Watson* the Court first determined whether the national measures in question constituted implementation of EU law in the sense of Article 51(1) of the Charter. To that effect, the Court looked, in the first place, at the scope of the ePrivacy Directive, as defined by Article 1(3) thereof, which excludes 'activities of the State' in specified fields, including the activities of the State in areas of criminal law and in the areas of public security, defence and State security, including the economic well-being of the State when the activities relate to State security matters. The Court noted however that Article 3 of Directive 2002/58 states that this Directive is to apply to the processing of personal data in connection with the provision of 'electronic communications services'. It further considered that, having regard to the general structure of the ePrivacy Directive, Article 15(1) necessarily presupposes that the national measures referred to therein, fall within the scope of that Directive. The Court therefore concluded that the ePrivacy Directive must be regarded as regulating the activities of the providers of such services, including those consisting in granting access to authorities to the retained data.

Secondly, the Court interpreted Article 15(1) of Directive 2002/58, in the light of Articles 7, 8, 11 and Article 52(1) of the Charter. It observed that, as stated in recital 2 thereof, that Directive seeks to ensure, in particular, full respect for the rights set out in Articles 7 and 8 of the Charter and that the EU legislature sought 'to ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used' (paragraph 82). The Court further observed that the principle of confidentiality of communications established by the ePrivacy Directive implies, inter alia, that, as a general rule, any person other than the users is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications. The only exceptions relate to persons

[114] Joined Cases C-203/15 *Tele2 Sverige AB v Post-och telestyrelsen* and C-698/15 *Secretary of State for the Home Department v Tom Watson and Others*, judgment of 21 December 2016, ECLI:EU: C:2016:970, not yet reported (*Tele2 Sverige*)

lawfully authorised in accordance with Article 15(1) of that directive and to the technical storage necessary for conveyance of a communication (paragraph 85).

Then the Court examined the compatibility of the national measures at issue, in the light of Articles 7, 8, 11 and 52(1) of the Charter. In this regard, the Court stressed that the concerned national legislation in the main proceedings covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, and does not provide for any differentiation, limitation or exception according to the objective pursued (paragraphs 97, 105 and 106). The Court also underlined that the interference entailed by such legislation in the fundamental rights enshrined in Articles 7 and 8 of the Charter is very far-reaching and must be considered to be particularly serious (paragraph 100). It concluded that such national legislation exceeds the limits of what is strictly necessary. Hence, it could not be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter (paragraph 107). The Court admitted, however that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary (paragraph 108).

On the specific issue of transfers of personal data to third countries, two important Cases should be signalled, the *Schrems* judgment[115] and Opinion A-1/15 on the transfer of *PN*R data to Canada[116].

In *Schrems*, the Court examined the validity of Commission Decision 2000/520 concerning the adequacy of protection of personal data transferred from the European Union to organisations established in the United States under 'the safe harbour' principles. The Court first noted that that Decision laid down that 'national security, public interest, or law enforcement requirements' had primacy over the safe harbour principles, and consequently self-certified United States organisations receiving personal data from the European Union were bound to disregard those principles without limitation where they conflicted with those requirements (paragraph 86). Second, the Court, referring to its case-law, in particular *Digital Rights Ireland*, recalled that legislation authorising, on a

[115] C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650 (*Schrems*).

[116] Opinion A-1/15, 26 July 2017, on the envisaged agreement between Canada and the European Union on the transfer of Passenger Name Record data (PNR) from the European Union to Canada, ECLI:EU:C:2017:592.

generalised basis, storage of all personal data without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail is not limited to what is strictly necessary (paragraph 93). Further, the Court held that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter (paragraph 95). The Court therefore declared Decision 2000/520 invalid.

A new adequacy decision was adopted by the Commission on 12 July 2016 on the EU-U.S. Privacy Shield[117].

Opinion of the Court A-1/15, delivered on 26 July 2017, was requested by the European Parliament, under Article 218 (11) of the TFEU, on the compatibility with the Treaties and the Charter of the envisaged PNR Agreement between the European Union and Canada as well as on the adequacy of the legal basis used.

On the legal basis, the Court held that the Council decision on the conclusion, on behalf of the Union, of the agreement between Canada and the European Union on the transfer and processing of PNR data must be based jointly on Articles 16(2) and 87(2)(a) TFEU (paragraphs 95 to 104).

In its analysis of the compatibility of the envisaged agreement with Articles 7, 8 and 52(1) of the Charter, the Court notes that the interferences with Articles 7 and 8 of the Charter consist in the systematic transfer of PNR data of all passengers from the European Union to Canada and its use, mainly, as 'an intelligence tool' (paragraph 130) as the PNR data transferred is, on the basis of the envisaged agreement, intended to be analysed systematically before the arrival of the aircraft in Canada by automated means, based on pre-established models and criteria, and verified automatically by cross-checking with other databases (paragraph 131).

Regarding the justification for the interferences resulting from the envisaged agreement, the Court held that the objective pursued by the envisaged agreement can justify limitations to fundamental rights. After reminding its case-law according to which rights under Articles 7 and 8 of the Charter are not absolute (paragraph 136), the Court then confirms its interpretation about the existence

[117] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p. 1.

of a right to security to be drawn from Article 6 of the Charter (paragraph 149) which is relevant in the context at stake. The Court also notes that the transfer of PNR data to Canada facilitates and expedites security and border control checks (paragraph 152). In the light of these considerations, the Court concludes that the transfer of PNR data to Canada and subsequent processing of that data may be regarded as being appropriate for the purpose of ensuring that the objective relating to the protection of public security and safety pursued by the envisaged agreement is achieved (paragraph 153).

However, on the strict necessity of the interference in relation with the categories of the PNR data referred to in the Annex to the envisaged agreement, and on whether that agreement laid down clear and precise rules governing the scope and application of the measures provided for, the Court considered that several provisions of the envisaged agreement were not limited to what is strictly necessary and did not lay down clear and precise rules. In particular, the Court found that the provisions of the agreement on the transfer of sensitive data to Canada and on the processing and retention of that data were incompatible with fundamental rights (paragraph 166). Similarly, the Court found that whereas storage of all PNR data during the air passengers' stay in Canada, and irrespective of the results of the automated analysis of the PNR data carried out prior to their arrival, was justified in order to combat terrorism and serious transnational crime. However, the continued storage of the PNR data of all air passengers after their departure from Canada was not limited to what is strictly necessary.

The Court therefore concluded that the envisaged agreement may not be concluded in its current form.

On 18 October 2017 the Commission submitted to the Council a Recommendation for a Decision to authorise the opening of negotiations for a revised Agreement with Canada[118] that should contain all the safeguards required in order for it to be compatible with the Charter as specified in the Opinion of the Court.

[118] COM(2017) 605 final.

NATIONAL REPORTS



AUSTRIA

Clemens Appl* • Philipp Homar** • Gabriel M. Lentner***
Thomas Ratka**** • Bettina Rinnerbauer*****

1. Binnenmarkt und elektronischer Handel: Internet und E-Kommerz

1.1. E-Kommerz und Verantwortlichkeit der Vermittlungsdiensteanbieter

Frage 1.1.1.

In Österreich wurde jüngst einiges an Kritik im Zusammenhang mit der Anwendung des Haftungsprivilegs des Host-Providers geübt.[1] Diese Kritik betrifft insbesondere Dienstleister, die auch als Inhaber eines elektronischen Mediums zu qualifizieren sind.[2] Nach *Staudegger* sei die ständige Rechtsprechung[3] zum Haf-

* Univ.-Prof. Ing. Dr. Clemens Appl, LL.M. ist Leiter des Department für Rechtswissenschaften und Internationale Beziehungen der Donau-Universität Krems.
** MMag. Philipp Homar ist wissenschaftlicher Mitarbeiter am Department für Rechtswissenschaften und Internationale Beziehungen der Donau-Universität Krems sowie wissenschaftlicher Mitarbeiter an der Abteilung für Informations- und Immaterialgüterrecht an der Wirtschaftsuniversität Wien.
*** Dr. Gabriel M. Lentner ist wissenschaftlicher Mitarbeiter am Department für Rechtswissenschaften und Internationale Beziehungen der Donau-Universität Krems.
**** Univ.-Prof. DDr. Thomas Ratka, LL.M. ist Vizerektor der Donau-Universität Krems sowie Fachbereichsleiter für Unternehmens-, Gesellschafts- und Kapitalmarktrecht.
***** Mag. Bettina Rinnerbauer ist wissenschaftliche Mitarbeiterin am Department für E-Governance in Wirtschaft und Verwaltung der Donau-Universität Krems.

[1] *Fötschl*, Das Haftungsprivileg des Host-Providers auf dem Prüfstand, MR 2015, 47 (49).

[2] § 1 Abs 1 Nr. 8 lit c MedienG. Voraussetzung ist eine "publizistische Funktion". Auch rein private Webauftritte können vom MedienG erfasst sein. Websites, die nur der Selbstdarstellung dienen, erfahren aber gewisse Begünstigungen (§ 1 Abs 1 Nr. 5a, § 21 MedienG). Die "gebotene Sorgfalt" im Sinne der entsprechenden Haftungstatbestände des MedienG gilt.

[3] OGH 21. 10. 2014, 4 Ob 140/14p (= MR 2015, 31 – "Fußballerfotos" [Uhl/Pateter; Walter]); 15. 12. 2014, 6 Ob 188/14m (= MR 2015, 19 – "Größter Verbrecher der 2. Republik"); 10. 4. 2014, 6 Ob 58/14v; 23. 1. 2014, 6 Ob 133/13x (= MR 2014, 59 – "E-Mail-Adresse des Posters").

tungsprivileg der Host-Provider für Website-Medieninhaber potentiell gefährlich für die Medienlandschaft.[4] Es entspräche der Intention des Gesetzgebers zur MedienG-Nov 2005[5], Medieninhaber von Host-Providern hinsichtlich ihrer Verantwortung streng zu trennen und die „gebotene Sorgfalt" (im Sinne der *Delfi* Entscheidung des EGMR[6]) nach MedienG[7] für Website-Betreiber zu verlangen.[8]

Die Judikatur scheint sich noch nicht speziell mit den verschiedenen Ansätzen zum MedienG im Zusammenspiel mit dem Haftungsprivileg des Host-Providers auseinandergesetzt zu haben.[9]

Frage 1.1.2.
Das Urteil des EuGH im Fall L'Oréal gegen eBay, C-324/09 erscheint durchaus sachgerecht. Das Problem der Verantwortlichkeit wird hierbei durchaus differenziert analysiert und letztlich in Richtung eines verstärkten Schutzes der Markeninhaber verstanden. Eine gewisse Problematik ist aber sehr wohl aus Sicht der Marktplatzbetreiber bei der praktischen Umsetzung zu erkennen. Im Ergebnis ist dieser restriktiven Handhabung der Providerprivilegien durchaus etwas abzugewinnen.[10]

Frage 1.1.3.
Das System von „notice-and-take-down" ist durchaus in der Lage und erfolgreich dabei Unrecht an der Quelle aufzufangen. Hierbei ist es möglich auch Ziele des Allgemeininteresses zu berücksichtigen, ohne auf eine effektive Rechtsdurchsetzung im Internet zu verzichten.[11]

Frage 1.1.4.
In Österreich wurde in diesem Zusammenhang die Beeinträchtigung von Persönlichkeitsrechten durch Bildnisveröffentlichung diskutiert. In einem Verfahren ging es um die „versehentliche" Veröffentlichung eines Bildes des Klägers,

[4] *Staudegger*, Medieninhaber als Hostprovider?, jusIT 2015/34, S. 86 (Heft 3 vom 18. 6. 2015). Ausführlich *Staudegger*, Haftungsprivilegierung des Hostproviders oder Medieninhaberschaft – tertium non datur, ALJ 2015, 42.

[5] BGBl I 49/2005. ErlRV 784, BlgNr 22. GP 6.

[6] EGMR 16.6.2015, Nr. 64569/09 (Großer Rat), MR-Int 2015, 53ff.

[7] §§ 6 Abs 2 Z 3a, 7 Abs 2 Z 5, 7a Abs 3 Z 5, 7b Abs 2 Z 4a und 7c Abs 2 iVm 7a Abs 3 Z 5 MedienG.

[8] *Staudegger*, Medieninhaber als Hostprovider?, jusIT 2015, 86. Ausführlich *Staudegger*, Haftungsprivilegierung des Hostproviders oder Medieninhaberschaft – tertium non datur, ALJ 2015, 42.

[9] *Fötschl*, Das Haftungsprivileg des Host-Providers auf dem Prüfstand, MR 2015, 47 (49).

[10] So auch Clemens Thiele, Der Marktplatzbetreiber als Mittelsperson: Was online gilt, gilt auch (fast) offline, Jus-IT 2016, 61ff.

[11] So wohl auch *Hofmann*, Das Allgemeininteresse an der Verfügbarkeit von Internet im Spannungsverhältnis zum Schutz von Urheberrechten, GPR 2017, 176, 179.

welches für einen Bericht über einen Selbstmörder verwendet wurde. In seinem Urteil fand der OGH deutliche Worte:

> „Im konkreten Fall haben die beanstandeten Lichtbildveröffentlichungen das Persönlichkeitsrecht des Klägers in hohem Maße beeinträchtigt. In der breiten Öffentlichkeit zu Unrecht als tot bezeichnet zu werden führt zu einer schwerwiegenden Kränkung. Zwar ist eine solche Behauptung – anders als oft der Vorwurf einer strafbaren Handlung – eher leicht widerlegbar. Dennoch konnte sich der Kläger über Monate nicht sicher sein, wer von seinen Bekannten ihn immer noch für einen (mittelbaren) Selbstmörder hielt. Darin liegt auch eine grobe Minderung seines sozialen Ansehens. Das Verschulden der Verantwortlichen in den Redaktionen der Beklagten, das bei der Bemessung des Schadenersatzes zu berücksichtigen ist (4 Ob 2059/96i = ÖBl 1996, 298 – Gerhard Berger II), wiegt schwer. Denn sie haben offenkundig auf gut Glück im Internet ein Foto zur Illustration ihrer Berichte gesucht, ohne sich darum zu kümmern, ob es tatsächlich die betroffene Person zeigte. Dass es dabei zu Verwechslungen kommen konnte, musste auch für sie auf der Hand liegen. Auf dieser Grundlage ist der jeweils geltend gemachte Anspruch auch unter Bedachtnahme auf die bereits im Medienverfahren zugesprochenen Entschädigungen angemessen."

Dennoch scheinen die Entschädigungen nicht in der Lage zu sein, die in Österreich gängige Praxis zu ändern, denn im gegenständlichen Verfahren wurde eine Entschädigung von lediglich 6.000 Euro für das Online-Medium festgelegt, was in keinem Verhältnis zu der hohen Verbreitung und Umsatzerlöse steht.[12]

Probleme stellen sich in der Praxis auch dann, wenn es darum geht, die Identität des Verfassers des persönlichkeitsverletzenden Postings zu eruieren. Hierbei ist man auf die Bereitschaft des Plattformbetreibers angewiesen (die Verpflichtung zur Auskunft nach § 18 Abs 4 ECG fällt in den koordinierten Bereich nach § 3 Z 8 ECG, daher gilt das Herkunftslandprinzip).[13]

Die Fragen 1.2.1-3. werden hier aus Zweckmäßigkeitsgründen gemeinsam behandelt. Das grundsätzliche Problem ist die Fragmentierung der Regelungen. Einerseits werden dadurch die Ziele (Förderung des Binnenmarktes, Verbraucherschutz) sowie die Kompetenzgrundlage (Art 114 AEUV) der Richtlinienentwürfe in Frage gestellt.[14] Andererseits bedeutet dies aus praktischer Sicht, dass ein Unternehmer jeweils vier Richtlinien und das anwendbare nationale Recht

[12] So auch *Thiele*, Persönlichkeitsschutz in Neuen Medien – Facebook, Google & Co, AnwBl 2013, 11 (13 f) mwN.

[13] *Thiele*, Persönlichkeitsschutz in Neuen Medien – Facebook, Google & Co, AnwBl 2013, 11 (13 f) mwN.

[14] *Lurger*, in *Wendehorst/Zöchling-Jud* (Hg) Ein neues Vertragsrecht für den digitalen Binnenmarkt? (2016) 41.

zu beachten hat, was gerade den europaweiten Handel erschwert.[15] Zu beachten ist weiters, dass es in Hinblick auf verspätete Leistungen sowie bei Teillieferungen noch dringenden Nachbesserungsbedarf gibt.[16]

1.2. Verbraucherschutz in Bezug auf das Internet und den E-Kommerz, Internet-Käufe und Vertragsrecht; Verbraucherschutz und Streitbeilegung

Frage 1.2.4.
Mit den genannten Verbraucherschutz-Regelungen kehrt die Europäische Kommission, zu einem sektorspezifischen Ansatz zurück. Hierbei werden einige wenige Fragen punktuell für einen engen Anwendungsbereich vollharmonisierend geregelt.[17] Das führt natürlich auch dazu, dass die Kohärenzproblematik auf die Ebene der Mitgliedstaaten verlagert wird und zu einer, wie schon erwähnten, Fragmentierung des Verbraucherschutzrechts führt. [18]

Frage 1.2.5.
Die Herausforderung für das Verbraucherschutzrecht angesichts der kollaborativen Wirtschaft liegt an den unklaren Grenzen zwischen Verbraucher und Unternehmen. Denn, obwohl die Betreiber der entsprechenden Plattform üblicherweise klar Gewerbetreibende im Sinne des Verbraucherschutzes sind, ist dies bei Dienstleistungserbringern weniger deutlich. Nach der Europäischen Kommission soll hierfür auf die Häufigkeit der Dienstleistungen, auf die Gewinnorientierung, sowie auf die Umsatzhöhe abgestellt werden. Dies erscheint zweckmäßig.

Frage 1.2.6.
In Österreich gab es einige Klagen, die sich gegen die von Online-Dienstanbietern angewandte Klauseln und Bedingungen richteten. Besonders hervorzuheben sind Fälle, die auch mediale Berichterstattung erfahren haben. Hierzu zählen insbesondere online-Partnervermittlungsportale, die oft Klauseln in ihren AGB enthalten, die dem Konsumentenschutzrecht zuwiderlaufen. Beispielsweise finden sich hier oft Bestimmungen, die eine automatische Verlängerung eines befristeten Vertrages beinhalten. Hier wurde vom Verein für Konsumenten

[15] *Winkler* in *Wendehorst/Zöchling-Jud* (Hg) Ein neues Vertragsrecht für den digitalen Binnenmarkt? (2016) 213-214.
[16] *Koch* in *Wendehorst/Zöchling-Jud* (Hg) Ein neues Vertragsrecht für den digitalen Binnenmarkt? (2016) 157.
[17] *Zöchling-Jud*, Gleiches Recht für alle? – UnGleichheiten im europäischen Rechtsraum aus dem Blickwinkel des Zivilrechts, AnwBl 2017, 357, 360-361.
[18] *Zöchling-Jud*, Gleiches Recht für alle? – UnGleichheiten im europäischen Rechtsraum aus dem Blickwinkel des Zivilrechts, AnwBl 2017, 357, 360-361.

Information ein Musterprozess geführt, der in zweiter Instanz Recht bekommen hat.

Ein weiteres Verfahren des österreichischen Vereins für Konsumenteninformation (VKI) wurde gegen die Geschäftsbedingungen des Online-Händlers Amazon eingeleitet. Die Verbandsklage wurde vom Handelsgericht stattgegeben, wurde aber dann vom Obersten Gerichtshof (OGH) dem EuGH vorgelegt, der das Urteil dahingehend revidierte, dass das US-Unternehmen Amazon in Europa als Amazon EU S.a.r.l. mit Sitz in Luxemburg aktiv ist und über eine Webseite im Internet einen Versandhandel betreibt, der sich auch an österreichische Kunden richtet. In Österreich besteht keine formelle Niederlassung. Daher habe das Recht des Sitzstaats des Unternehmens, bei Rechtswahl durch das Unternehmen Vorrang gegenüber dem Recht des Konsumentenstaates (mit Ausnahme der zwingenden Verbraucherschutzregeln).

Frage 1.2.7.
Ein solcher Ansatz würde den Grundwertungen des österreichischen Unternehmensrechts, das die Abgrenzung aus Gründen der Rechtssicherheit formal zieht (§ 343 UGB) widersprechen und ist uE aus systematischen Erwägungen daher abzulehnen.

1.3. Geoblocking

Frage 1.3.1.
Artikel 1 Abs 5 des Kommissionsvorschlages sieht explizit vor, dass die Anwendung der VO impliziert, dass der betreffende Anbieter automatisch die Voraussetzungen für den Verbrauchergerichtsstand nach VO 1215/2015 erfüllt. Der Vorschlag greift daher nicht in die Zuständigkeitsregelungen der VO 1215 ein und lässt diese unverändert.

1.4. Fragen in Bezug auf die kollaborative Wirtschaft

Frage 1.4.1.
Im Zusammenhang mit der kollaborativen Wirtschaft gab es in Österreich einige Gerichtsstreitigkeiten. Beispielsweise klagten zwei Wiener Taxiunternehmer Mietwagen-Unternehmer, die für das Fahrten-Vermittlungs-Unternehmen Uber tätig sind. Vor dem Handelsgericht Wien wurde eine einstweilige Verfügung erwirkt. Das Urteil ist nicht rechtskräftig. Uber ist als Vermittler zu qualifizieren, da es weder eigene Fahrer beschäftigt noch eigene Fahrzeuge besitzt. Der Beförderungsvertrag wird daher mit einem selbständigen Mietwagenunternehmer abgeschlossen, für die über eine Vermittlungsgebühr von den Fahrtkosten behält.[19]

[19] *Mahr/Dechant*, Taxischreck Online-Fahrdienstvermittler, ÖJZ 2016, 398, 399.

Es stellt sich hier die Frage nach der Rechtmäßigkeit, insbesondere im Hinblick auf die Bestimmungen der Gewerbeordnung (GewO), des Gelegenheitsverkehrsgesetzes (GelverkG) sowie der Betriebsordnung für den nichtlinienmäßigen Personenverkehr (BO 1994) und die Wiener Taxi-, Mietwagen- und Gästewagen-Betriebsordnung (BO Wien).[20]

Auch die Stadt Salzburg ging gegen Vermittlungsplattformen wie Airbnb, wimdu oder 9flats vor.

In einer richtungsweisenden Entscheidung, kam der OGH in einer sehr kurz gehaltenden Begründung zum Schluss, dass eine Umwidmung einer zu Wohnzwecken genutzen Wohnung in ein Ferienappartement für Touristen der Zustimmung aller Wohnungsbesitzer im Haus bedurft.[21]

Frage 1.4.2.

Wettbewerbsprobleme ergeben sich auf verschiedenen Ebenen. Von Seiten der Hoteliervereinigung wird beispielsweise auf eine mangelnde Chancengleichheit hingewiesen, weil Sharingplattformen in einem rechtlichen Graubereich agieren, um „Kosten für Mitarbeiter zu vermeiden", diese Plattformen müssen auch, anders als bei Hotels, keine Betriebsanlagengenehmigung einholen und auch nicht alle kosten für die Kunden preislich auszeichnen. Auch abgabenrechtlich seien diese nicht gleichgestellt, da Plattformen üblicherweise die Ortstaxe oder 13 Prozent Steuern zahlen würden.

Auch bei online-Fahrtenvermittlern wie Uber stellt sich die arbeits- und sozialrechtliche Frage inwieweit Uber-Fahrer als selbständige Auftragnehmer oder doch als Angestellte anzusehen sind.[22] Ein fairer Wettbewerb scheint dadurch gefährdet, da, wenn ein Unternehmen im Gegensatz zu Mitbewerbern keine Steuern abführt, der Fahrpreis immer niedriger ausfallen wird.

Auch könnte Uber als Fahrdienstvermittler gegen Kartellrecht verletzen, dadurch, dass einheitliche Preise für alle Anbieter festgelegt werden.[23]

Auch die Nichteinhaltung öffentlich-rechtlicher Bestimmungen kann ein Wettbewerbsvorsprung vor gesetzestreuen Mitbewerbern darstellen. Es ist daher möglich, dass solche Verstöße einen spürbaren Wettbewerbsverstoß darstellen.[24]

[20] *Mahr/Dechant*, Taxischreck Online-Fahrdienstvermittler, ÖJZ 2016, 398, 399.

[21] OGH 23.04.2014, 5Ob59/14h wobl 2014,209/78 (Etzersdorfer) – wobl 2014/78 (Etzersdorfer) = VbR 2014/104 S 169 – VbR 2014,169 = Der Mieter 2014,27 = Zak 2014/403 S 217 – Zak 2014,217 = Prader/Markl, Zak 2014/620 S 323 – Prader/Markl, Zak 2014,323 = MietSlg 66.48. Siehe auch http://derstandard.at/2000002770991/OGH-schiebt-Airbnb-Co-Riegel-vor abgerufen 28.9.2017.

[22] *Mahr/Dechant*, Taxischreck Online-Fahrdienstvermittler, ÖJZ 2016, 398, 399.

[23] *Mahr/Dechant*, Taxischreck Online-Fahrdienstvermittler, ÖJZ 2016, 398, 399.

[24] *Mahr/Dechant*, Taxischreck Online-Fahrdienstvermittler, ÖJZ 2016, 403.

Frage 1.4.3.
Siehe dazu zu Frage 1.4.5.

Frage 1.4.4.
Das Verbraucherschutzrecht der EU (sowie auch das Lauterkeitsrecht) setzt eine klare Unterscheidung zwischen Verbrauchern einerseits und Gewerbetreibenden andererseits voraus. Dieser Differenzierung liegt der Gedanke zu Grunde, dass bei Verbrauchergeschäften, der Gewerbetreibende regelmäßig die stärkere Partei ist, vor der die schwächere Partei geschützt werden muss. In der kollaborativen Wirtschaft, ist eine solche Grenzziehung oftmals schwer zu treffen. Meist klar ist, dass die Plattformbetreiber Gewerbetreibende im Sinne des Verbraucherschutzrechts sind.

Aus verbraucherschutzrechtlicher Sicht, ist sodann nicht immer klar welche Rechte dem Verbraucher als Kunden zustehen. Zum Beispiel unterliegt eine Buchung über die Plattform „Airbnb", wenn diese als Mietvertrag eingestuft wird, dem Recht jenes Staates, in dem sich die Wohnung befindet. Auch bei innerösterreichischen Sachverhalten stellt sich die Frage ob das Konsumentenschutzrecht anwendbar ist, denn dieses greift nur dann, wenn der Vermieter der Wohnung als Unternehmer zu qualifizieren ist.

Frage 1.4.5.
Aus Platzgründen können hier nicht die einzelnen „Peer-to-Peer"-Dienstleistungen auf die Frage unter welchen Umständen diese der österreichischen Gewerbeordnung unterliegen, überprüft werden. Entscheidend ist, dass die Abgrenzung hier auf die konkreten Umstände des Einzelfalles abzustellen ist. Ein praktisch wichtiges Beispiel ist die der privaten Raumvermietung samt Inventar. Dies würde nicht der Gewerbeordnung unterliegen. Jedoch wäre die Anwendung der Gewerbeordnung dann zu prüfen, wenn zusätzlich Bettwäsche und Handtücher getauscht werden und ein Frühstück angeboten wird.

Frage 1.4.6.
Anders als bei B2C-Modellen, ist für „Peer-to-Peer"-Diensten zwischen Mitgliedern einer Sharing-Gemeinschaft Vertrauen wichtig. Hierfür ist ein System erforderlich, dass Mitgliedern (aber auch nur diesen) erlaubt durch Referenzen und Bewertungen ihre Reputation aufzubauen.

Alleine auf online-rating gestützt ist ein Missbrauch von darauf gestütztem Vertrauen nicht auszuschließen.[25] Daher scheint es sinnvoll, gewisse Verifizier-

[25] Dazu *Seidelberger*, Bewertungen auf Internetplattformen: Die Grenzen der Zulässigkeit, ipCompetence 2015, 28.

ungen einzuführen, damit das Vertrauen der Verbraucher darauf nicht erschüttert wird.

Ein sinnvoller Beitrag hierzu könnten staatliche Behörden leisten, die nach Vorbild ähnlicher Behörden in vielen Staaten, wie zum Beispiel der Federal Trade Commission in den USA, der Competition and Market Authority in Großbritannien, oder die Autorità Garante della Concorrenza e del Mercato in Italien, organisiert sind. Diese Behörden sind sowohl für die Überwachung des Wettbewerbs als auch für Verbraucherschutz und das Lauterkeitsrecht zuständig.

2. Digitale Media

Frage 2.1.

Nach der Spruchpraxis der KommAustria handelt es sich bei redaktionell aufbereiteten Text-, Video- oder Bildbeiträgen aus unterschiedlichen Themenbereichen, die von einem Zeitungsverlag in einem Internetportal bereitgestellt werden, um „Sendungen" im Sinne des § 2 Z 30 Bundesgesetz über audiovisuelle Mediendienste (Audiovisuelle Mediendienste-Gesetz – AMD-G)[26]. Bezüglich der Beurteilung, ob es diese Beiträge den Begriff der „Sendung" erfüllen, kommt es darauf an, „ob das audiovisuelle Angebot (losgelöst von anderen Angeboten desselben Anbieters) eine eigenständige Funktion erfüllt und nicht nur eine Begleitung oder Ergänzung zu einem Textangebot darstellt"[27]. Dass diese Beiträge unter einer Subdomain der Printzeitung angeboten werden, ändert nichts an deren Eigenständigkeit, sofern das Videoportal unabhängig vom Rest des Webauftritts nutzbar ist und ohne Einbettung in den gesamten Webauftritt angeboten werden könnte.[28]

Da die besprochenen Entscheidungen bereits vor dem ggst. Urteil des EuGH ergangen sind, hat dieses keine unmittelbare Änderung der österreichischen Spruchpraxis erfordert.

Frage 2.2.

Grundsätzlich ist es zu begrüßen, Anbieter von Angebotsformen, die im Zuge der Medienkonvergenz zunehmend dieselben Bedürfnisse der Konsumenten befriedigen, einheitlichen Regelungen zu unterstellen. Zu begrüßen ist auch, einen klaren Rechtsrahmen über die Verantwortung und Verpflichtung von Content-Plattformen bezüglich Hassreden und des Schutzes von Minderjährigen zu

[26] siehe die Bescheide der KommAustria vom 11.4.2014, KOA 1.950/14-026, abrufbar über https://www.rtr.at/de/m/KOA195014026/32057_KOA_1.950-14-026.pdf, KOA 1.950/14-027, abrufbar über https://www.rtr.at/de/m/KOA195014027/32058_KOA_1.950-14-027.pdf sowie vom 17.6.2013, KOA 1.950/13-044, abrufbar über https://www.rtr.at/de/m/KOA195013044/29848_KOA_1.950-13-044.pdf).

[27] KOA 1.950/14-026, S. 7 sowie KOA 1.950/14-027, S. 7.

[28] KOA 1.950/14-026, S. 8 sowie KOA 1.950/14-027 S. 8.

schaffen. Diesbezüglich ist jedoch zu beachten, dass sich Content-Plattformen (wie bspw YouTube) von herkömmlichen Programmanbietern unterscheiden, indem der Großteil der Inhalte von den Nutzern erstellt und hochgeladen wird. Eine stärkere Regulierung dieser Plattformen ist insofern kritisch zu sehen, als eine solche mit der Verpflichtung zur Implementierung von vorbeugenden Filtermechanismen zur Inhalteerkennung einhergeht. Dies würde sowohl Bedenken hinsichtlich einer Zensur hervorrufen, zumal eine verstärkte Verantwortung der Plattformen auch Anreize setzt, die von den Nutzern bereitgestellten Inhalte im Zweifel zu sperren oder gar nicht erst freizuschalten. Zudem würde dies dem derzeit geltenden Haftungsregime (Art 15 RL 2000/31/EG) widersprechen, wonach Hosting-Plattformen keinen allgemeinen Überwachungspflichten unterworfen werden dürfen. Nach der Rechtsansicht der KommAustria können Nutzer von Content-Plattformen, welche audiovisuelle Inhalte bereitstellen, bereits nach derzeitiger Rechtslage unter die medienrechtlichen Bestimmungen des AMD-G fallen und folglich Melde-, Kennzeichnungs- und Regulierungspflichten unterliegen; aufgrund eines veröffentlichten Berichts dürften Verstöße bisher aber noch nicht verfolgt worden sein.[29]

Frage 2.3.
Auf Basis der veröffentlichten Entscheidungen der Regulierungsbehörden sind keine Fälle bekannt.

Frage 2.4.
Gemäß § 6 Abs 1 AMD-G sind die Mitglieder der KommAustria in der Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden. Somit ist die österreichische Regulierungsbehörde bereits zum derzeitigen Stand als weisungsfreie Behörde eingerichtet. Die Weisungsfreiheit ist insofern zu begrüßen, als die Wahrnehmung der aufsichtsbehördlichen Aufgaben (insb der Kampf gegen Hassreden, die Regulierung der gewerblichen Kommunikation aber auch die Aufsicht über den österreichischen Rundfunk) aus demokratiepolitischen Gründen unabhängig von einem Einfluss durch politische Parteien zu erfolgen hat. Aus diesem Grund kann die bereits derzeit bestehende österreichische Einrichtung der Regulierungsbehörde als Benchmark für die rechtspolitische Gestaltung auf EU-Ebene herangezogen werden. Fälle von unlauterem politischen oder wirtschaftlichen Druck auf die Medienregulierungsbehörde sind nicht bekannt.

Frage 2.5.
Nach § 2 Z 27 AMD-G handelt es sich bei Produktplatzierung um „jede Form audiovisueller kommerzieller Kommunikation, die darin besteht, gegen Entgelt

[29] http://www.horizont.at/home/news/detail/kommaustria-und-rtr-nehmen-youtube-ins-visier.html

oder eine ähnliche Gegenleistung ein Produkt, eine Dienstleistung oder eine entsprechende Marke einzubeziehen bzw. darauf Bezug zu nehmen, so dass diese innerhalb einer Sendung erscheinen". Das für den österreichischen Rundfunk geltende ORF-G[30] sieht eine inhaltlich entsprechende Definition einer Produktplatzierung vor (vgl § 1a Z 10 ORF-G). Nach § 16 Abs 5 Z 3 ORF-G bzw § 38 Abs 4 Z 3 AMD-G dürfen Sendungen, die Produktplatzierungen enthalten, das betreffende Produkt nicht zu stark herausstellen.

Diesbezüglich hat der Verwaltungsgerichtshof entschieden, dass es für das Vorliegen einer Produktplatzierung nach § 1a Z 10 ORF-G nicht darauf ankommt, dass für diese tatsächlich ein Entgelt geleistet wurde; vielmehr kommt es darauf an, dass eine Platzierung nach der Verkehrsauffassung üblicherweise gegen Entgelt erfolgt.[31]

Einzelfallbezogene Entscheidungen existieren bezüglich Verstöße gegen die zum Schutz von Minderjährigen bestehende Bestimmung des § 42 AMD-G (Gefährdung der körperlichen, geistigen oder sittlichen Entwicklung von Minderjährigen aufgrund einer Ausstrahlung unsittlicher Inhalte zu Sendezeiten, wo diese üblicherweise auch von Minderjährigen wahrgenommen werden[32], sowie gegen das Verbot der Schleichwerbung des § 31 Abs 2 AMD-G verstoßen[33].

Frage 2.6.

Im DSG[34] und KommAustria-G[35] sind keine Bestimmungen über eine Zusammenarbeit der Datenschutzbehörde und der Medienregulierungsbehörde enthalten. Eine enge inter-behördliche Zusammenarbeit ist freilich zu begrüßen, doch sollte berücksichtigt werden, dass den Einrichtungen unterschiedliche Aufgaben obliegen und der Datenschutzbehörde in Datenschutzbelangen eine gewisse Aufsichtsfunktion über die behördliche Tätigkeit der anderen Behörden obliegt. Zur umfassenden Evaluierung des Marktverhaltens von Medienanbietern, wäre ein gemeinsames Vorgehen von medienrechtlicher und datenschutzrechtlicher Aufsicht wünschenswert. Soweit ersichtlich gibt im Schrifttum dazu keinen näheren Ausführungen.

[30] Bundesgesetz über den Österreichischen Rundfunk BGBl. Nr. 379/1984 idgF.

[31] VwGH 28.2.2014, 2012/03/0019.

[32] siehe Bescheid der KommAustria vom KOA 4.400/13 – 009, abrufbar über https://www.rtr.at/de/m/KOA440013009/30286_KOA_4.400-13-009.pdf.

[33] Bescheid der KommAustria vom 11.7.2017, KOA 2.250/17-009, abrufbar über https://www.rtr.at/uploads/media/36071_KOA%202.250-17-009.pdf.

[34] Bundesgesetz über den Schutz personenbezogener Daten BGBl. I Nr. 165/1999 idgF.

[35] Bundesgesetz über die Einrichtung einer Kommunikationsbehörde Austria BGBl. I Nr. 32/2001 idgF.

Frage 2.7.
Die Bestimmungen sind nach wie vor in Kraft, vgl § 17b UrhG, wonach eine Rundfunksendung über Satellit (vorbehaltlich des Abs 2 leg cit) nur in dem Staat stattfindet, in dem die Eingabe vorgenommen wird. Bisher erfolgte keine Anwendung des Sendlandprinzips auch auf Online-Übertragungen.

Frage 2.8.
Bisher stellten das urheberrechtliche Territorialitätsprinzip sowie die territorial gesplittete Rechtewahrnehmung die maßgeblichen Hindernisse für die Portabilität der Inhalte dar. Es bleibt abzuwarten, inwiefern sich dies in Zukunft durch den Verordnungs-Entwurf COM(2015) 627 final ändern wird. Eine gewisse Überprüfung des Ursprungslandprinzip wird auch nach dem VO-Entwurf zulässig sein (vgl Art 5 Abs 2 COM(2015) 627 final); um dem unterschiedlichen Preisniveau der Staaten Rechnung zu tragen, ist es grundsätzlich auch gerechtfertigt, eine gewisse Anknüpfung des Verbrauchers an den jeweiligen Staat zu verlangen, nach dem sich der Dienst richtet (so dies auch bei der Regelung über die Roaminggebühren in der EU erfolgte). Im Fall einer Überprüfung muss diese jedenfalls in vollem Umfang den Datenschutzbestimmungen (die entsprechenden Reformvorschläge lassen die datenschutzrechtlichen Vorgaben unberührt) entsprechen, was eine Zustimmung des Verbrauchers voraussetzen wird.

3. Digitale Infrastrukturen

Frage 3.1.
Vor der Verordnung 2015/2120 gab es in Österreich keine Regelungen zur Neutralität im Internet.[36]

Zu „zero-rating" hat sich der österreichische Telekom-Regulator (RTR) enttäuscht gezeigt über die Tatsache, dass diese Praktiken nicht ausdrücklich verboten sind. Aus Sicht des RTR ist damit „langfristig die Netzneutralität und die Innovationskraft des Internet massiv gefährdet".[37]

Aus Behördensicht ist auffällig, dass „derzeit in erster Linie klare und eindeutige Verstöße gegen die Netzneutralität wie technische Diskriminierungen, z.B. Zero-Rating außerhalb des Data Caps, geahndet [werden]". „Nach einem zögerlichen Start gewinnt der Vollzug der Netzneutralitätsverordnung in einigen thematischen Hot Spots (etwa Zero-Rating) nunmehr Momentum,

[36] *Hödl*, Zur Frage der gesetzlichen Festschreibung der Netzneutralität, jusIT 2010, 201; Feiler/Stahov, Rechtliche Aspekte der Netzneutralität und ihrer Einschränkung, Medien und Recht 2011, 287.
[37] derstandard.at/2000024675021/Telekom-Regulator-sieht-Netzneutralitaet-massiv-gefaehrdet abgerufen 28.9.2017.

ohne dabei aber die einheitliche europäische Perspektive aus den Augen zu verlieren."[38]

Frage 3.2.
Österreich hat eine über die Ziele der Digitalen Agenda für Europa (DAE) hinausgehende Breitbandstrategie verabschiedet, nach der eine vollständige Abdeckung mit ultraschnellem Breitbandinternet bis 2020 verwirklicht werden soll. Zur Erreichung dieses Ziels, wird ein Fokus auf den marktgetriebenen Ausbau gelegt und ländliche Regionen werden speziell durch öffentliche Förderprogramme unterstützt, da für sie keine privaten Investitionen getätigt werden. Die staatliche Breitband-Förderung wurde aber auch aufgrund ihrer vermeintlichen wettbewerbsverzerrender Wirkung kritisiert.[39]

Frage 3.3.
Hierzu gibt es soweit ersichtlich keine Diskussionen im Schrifttum.

Frage 3.4.
Die Kommunikationsmärkte in Österreich werden durch mehrere nationale Regulierungsbehörden im Bereich der Telekommunikation und des Rundfunks reguliert. Dazu zählen die Bundesministerin für Verkehr, Innovation und Technologie, die Oberste Fernmeldebehörde (geleitet vom BM), die Fernmeldebüros, die RundfunkundTelekom Regulierungs-GmbH (RTR), die Telekom-Control-Kommission (TKK), die Kommunikationsbehörde Austria (KommAustria) und den Bundeskommunikationssenat (BKS).

Vor dem 1.10.2010 entsprachen nur die TKK und der BKS (als Behörde mit richterlichem Einschlag gem Art 133 Ziffer 4 B-VG) dem Kriterium der Unabhängigkeit im Sinne des Art 3 RahmenRL. Mit 1.10.2010 (KommAustria Gesetz-Novelle) ist auch die KommAustria gemäß Art 20 Abs 2 Z 5a B-VG iVm § 6 Abs 1 KOG unabhängig und weisungsfrei.

4. Daten in der digitalen Wirtschaft

Frage 4.1.
Entgegen der ursprünglichen Absicht, ein neues Datenschutzgesetz zu erlassen und das geltende DSG 2000 aufzuheben, die der Regierungsvorlage zu entnehmen ist[40], wurde das Bundesgesetz über den Schutz personenbezogener Daten

[38] https://www.rtr.at/de/inf/KBericht2016/K-Bericht_2016.pdf
[39] http://www.nachrichten.at/nachrichten/wirtschaft/Die-Breitband-Milliarde-ist-eine-Wettbewerbsverzerrung;art15,2278081
[40] ErlRV BlgNR 1664, XXV. GP, S. 2.

(Datenschutzgesetz 2000 – DSG 2000), BGBl I 165/1999 idF BGBl I 132/2015 auf Grund der VO (EU) 2016/679, ABl. Nr. L 119 vom 4.5. 2016 S. 1 (Datenschutz-Grundverordnung oder kurz „DSG-VO"), und zur Umsetzung der Richtlinie (EU) 2016/680, ABl Nr. L 119 vom 4.5.2016 S. 89[41] durch das Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (Datenschutz-Anpassungsgesetz 2018), BGBl I 120/2017[42], angepasst.

Im Schrifttum wurden insbesondere die zeitlichen Rahmenbedingungen im Zuge der Erlassung des Gesetzes diskutiert. Der *Verein für Konsumenteninformation* kritisierte beispielsweise die kurze Zeitspanne vom Ablauf der Begutachtungsfrist zum Ministerialentwurf bis zur Verabschiedung der Regierungsvorlage (23.06.2017-29.06.2017), welche „im Wesentlichen unverändert" erfolgt sei.[43] Für *Lehofer* wirkte die Beschlussfassung über das Datenschutz-Anpassungsgesetz 2018 „etwas überstürzt".[44] *Knyrim* ist der Ansicht, dass von über 100 eingelangten Stellungnahmen im Text selbst nur wenige aufgegriffen worden seien.[45] *Anderl/Tlapak* sehen in der raschen Erlassung des Datenschutz-Anpassungsgesetzes 2018 einerseits den Vorteil nun vorliegender Orientierungspunkte für Unternehmen, sowie andererseits etwa den potentiellen Nachteil möglicher Rechtszersplitterung durch Regelungen in Materiengesetzen.[46]

Nach *Asen* wurde die in der Regierungsvorlage vorgeschlagene Neuformulierung des Grundrechts auf Datenschutz sowie die ebendort vorgeschlagene Änderung der Kompetenzverteilung hin zu einer alleinigen Kompetenz des Bundes in Bezug auf Gesetzgebung und Vollziehung allgemeiner Angelegenheiten des Schutzes personenbezogener Daten nicht weiter verfolgt, weil zweifelhaft gewesen sei, ob das hierfür erforderliche Konsensquorum (2/3) im Nationalrat erreicht worden wäre. Als Konsequenzen zeigt *Asen* die Weitergeltung sowohl des Grundrechts in der Form des geltenden DSG 2000 als auch die Beibehaltung der zwischen Bund und Ländern geteilten Zuständigkeit in Bezug auf allgemeine Angelegenheiten des Datenschutzes auf. Es sind weiterhin Landesgesetze für Fälle des nicht automationsunterstützten Datenverkehrs maßgeblich.[47] Dies wurde offenbar nicht als die zweckmäßigste Lösung betrachtet: Nach den Erläuterungen zur genannten Regierungsvorlage sei

[41] ErlRV BlgNR 1664, XXV. GP, S. 1 https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_01664/fname_640101.pdf (abgerufen am 19.09.2017).

[42] Weitere Informationen zum Datenschutz-Anpassungsgesetz 2018: https://www.ris.bka.gv.at/eli/bgbl/I/2017/120 (abgerufen am 19.09.2017).

[43] Datenschutz-Anpassungsgesetz 2018: Lücken im Rechtsschutz, VRInfo 2017 H 6, 23.

[44] *Lehofer*, H.P. (2017), Parlamentskehraus, ÖJZ 2017/85.

[45] Rainer *Knyrim*, Neues Österreichisches Datenschutzgesetz final beschlossen!, Dako 2017/47.

[46] *Anderl, A./ Tlapak, N.* (2017), Vorbereitung auf die DSGVO europaweit in den Kinderschuhen, Dako 2017/52 (84).

[47] *Asen*, S. (2017), Kundmachung: Datenschutz-Anpassungsgesetz 2018, AnwBl 2017, Heft 9/2017, 476.

es unzweckmäßig, dass die Zuständigkeit zur Gesetzgebung betreffend automationsunterstützte Datenverarbeitung beim Bund und betreffend manuelle Datenverarbeitung bei den Ländern liegen soll, zumal der in der Vergangenheit durch RL 95/46/EG vorgegebene und durch § 1 DSG 2000 determinierte „Gestaltungsspielraum äußerst gering gewesen sei."[48]

Ein weiteres interessantes Charakteristikum des Datenschutz-Anpassungsgesetzes 2018 ist die im Vergleich zu Art 8 Abs 1 DSG-VO (vollendetes 16. Lebensjahr) niedrigere Altersgrenze als Voraussetzung für eine zulässige Einwilligung durch das Kind (§ 4 Abs 4 DSG: vollendetes 14. Lebensjahr).[49]

Aus arbeitsrechtlicher Sicht wurden die Beibehaltung der Regelung von Beschäftigtendatenschutz in den arbeitsrechtlichen Materiengesetzen (z.B. ArbVG) sowie der Schutz der betrieblichen Interessensvertretungen hervorgehoben.[50]

Neben diesen legistischen Maßnahmen wurde von der Datenschutzbehörde ein Leitfaden zur DSGVO zur Verfügung gestellt, welcher das Wissen der MitarbeiterInnen zum angegebenen Zeitpunkt (Juli 2017) zusammenfassen soll.[51]

Frage 4.2.

Um diese Frage einer substantiellen Beantwortung zuzuführen, wäre die Befragung für die österreichische Wirtschaftslandschaft repräsentativer Unternehmen vonnöten. In Ermangelung derartiger empirischer Daten, sollen Aussagen des Gesetzgebers im Rahmen der Wirkungsorientierten Folgenabschätzung als Ausgangspunkt für Einblicke in Anpassungsbedarf auf Seiten der Unternehmen dienen.

Gemäß den Ausführungen im Rahmen der Wirkungsorientierten Folgenabschätzung anlässlich der Änderungen des DSG, seien dadurch „keine wesentlichen Auswirkungen auf die Verwaltungslasten für Unternehmen" zu erwarten. Es wird davon ausgegangen, dass die Auskunft über die Identität des Verantwortlichen von Unternehmen 100x pro Jahr für 30 Minuten verlangt würde. Darüber hinaus wird als wesentliche Auswirkung angenommen, dass 8000 Unternehmen ihre MitarbeiterInnen etwa über Folgen der Verletzung des Datengeheimnisses neu belehren werden müssen.[52]

[48] ErlRV 1664 BlgNR, XXV. GP, S. 2 (zu Z 1 bis 3).

[49] *Anderl, A./ Tlapak, N.* (2017), Vorbereitung auf die DSGVO europaweit in den Kinderschuhen, Dako 2017/52 (83). Von denselben wird auch darauf hingewiesen, dass die Grenze des Art 8 Abs 1 DSG-VO in einem früheren Entwurf beibehalten werden sollte.

[50] *Ercher-Lederer*, G. (2017), Datenschutz-Anpassungsgesetz 2018 und Beschäftigtendatenschutz, ASoK 2017, 315.

[51] *Schmidl*, M. (2017), Verordnung (EU) 2016/679 –Datenschutz-Grundverordnung, S. 3. Siehe https://www.dsb.gv.at/documents/22758/116802/DSGVO-2016-Leitfaden.pdf/93d6cb80-8d8e-433d-a492-a827e3ed81a2 (abgerufen am 19.09.2017).

[52] WFA zu RV BlgNR 1664, XXV. GP, S. 9 https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_01664/fname_640100.pdf (abgerufen am 19.09.2017).

Es kann davon ausgegangen werden, dass Unternehmen Beratungsleistungen, insbesondere solche der Interessenvertretung der Wirtschaftstreibenden, in Anspruch nehmen. Verschiedene Interessenvertretungen bieten Informationen zur DSGVO an. Zum einen offeriert die Wirtschaftskammer Österreich (WKO) nähere Informationen („Checkliste" und „TO DO Liste") zur DSGVO[53], zum anderen wurden unter anderem auch von der Arbeiterkammer in Zusammenarbeit mit gewerkschaftlichen Vertretern Informationsveranstaltungen abgehalten[54]. Darüber hinaus erkennt auch die Unternehmensberatung Information im Zusammenhang mit der DSG-VO als Geschäftsfeld und bewirbt entsprechende Angebote.[55]

Als zusätzliche Informationsquelle kann den UnternehmerInnen auch wissenschaftliche und Fachliteratur dienen. Neben der Auseinandersetzung mit der DSGVO mit dem Ziel der Generierung einer Übersicht[56] sind der Literatur Überlegungen dazu zu entnehmen, nach welchem Vorbild eine Datenschutz-Folgenabschätzung erfolgen könnte[57], auch wurden zu beachtende Punkte in Listenform dargestellt[58] und die Frage nach der Bestellung eines Datenschutzbeauftragten mit Empfehlungen für die Praxis verbunden[59]. Im Zusammenhang mit der Beschreibung eines an die Erfordernisse der DSGVO anzupassenden Datenmanagement-Systems stellen *Leiter/Pollirer* fest, dass es in Österreich an Erfahrung mit Datenschutzbeauftragten fehle und verweisen auf zwei Gesetzesvorhaben zur freiwilligen bzw. verpflichtenden Bestellung eines Datenschutzbeauftragten, welche nicht umgesetzt worden seien.[60]

Frage 4.3.

In der Literatur wurden unterschiedliche Kriterien, etwa technologische, menschliche und institutionelle Faktoren, dafür vorgeschlagen, was eine Stadt zur Smart City machen soll.[61] Eng mit dem Begriff „Smart City"

[53] https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Checkliste.html sowie https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Auswirkungen-auf-Websites.html

[54] Knyrim, R./ Schmidt, K., Der gläserne Mitarbeiter ist schon Realität, Dako 2017/31 (50).

[55] Z.B. https://home.kpmg.com/at/de/home/insights/2017/06/in-2017-dsgvo.html oder https://www2.deloitte.com/at/de/seiten/analytics/articles/eu-datenschutzgrundverordnung-loesungsansatz.html

[56] *Gruber*, J. P. (2017), Die Datenschutz-Grundverordnung im Überblick , ASoK 2017, 243 (243)

[57] *Pollirer*, H.-J. (2015), Die Datenschutz-Grundverordnung: Die Datenschutz-Folgenabschätzung (Teil III), Dako 2015/47 (88).

[58] *Graf, F./ Križanac*, M. (2017), DS-GVO Compliance , ecolex 2017, 925.

[59] *Schweiger*, T., Benötigt Ihr Unternehmen ab 25. 5. 2018 einen Datenschutzbeauftragten? (Teil X), Dako 2017/20 (34).

[60] *Leiter, M./ Pollirer*, H.-J., Praxisprojekt: Das Datenschutz-Management-System (DSMS) bei den Österreichischen Bundesbahnen (ÖBB), Dako 2017/18 (29).

[61] Siehe z.B. *Taewoo, N./Pardo*, T. A. (2011), Conceptualizing Smart City with Dimensions of Technology, People, and Institutions, Proceedings of the 12th Annual International Conference on Digital

verbunden[62] ist Internet Of Things oder „Internet der inge", as miteinschließt, dass „mit Hilfe digital arbeitender Werkzeuge der Zustand von realen "Dingen" erfasst und dieser für die Weiterverarbeitung dieser Dinge im Internet zur Verfügung gestellt wird."[63]

Als wesentliches Merkmal des Internet Of Things erscheint das Interagieren von Menschen und Maschinen oder (auch) von Maschinen mit Maschinen. Dies kann in verschiedenen Bereichen des Lebens in Betracht kommen wie etwa im Verbrauchergeschäft, im Straßenverkehr und im privaten Wohnbereich. Von besonderem Interesse sind regelmäßig Fragen nach den Rechten der Nutzer an beteiligten Dingen sowie nach dem Verantwortlichen im Fall eines Schadenseintritts.

Im Allgemeinen ist die konkrete vertragliche Vereinbarung maßgeblich bzw. die Frage welcher Vertragspartner welche Leistung schuldet, um die Rechtspositionen der Beteiligten wie etwa im Hinblick auf die Haftung für Schäden zu eruieren; durch eine strafrechtswidrige, schuldhafte Handlung einer Person kann eine strafrechtliche Haftung hinzutreten (wie beispielsweise falsche Bedienung eines Ambiant Assisted Living Systems).[64]

Maßgeblich ist die Frage, ob es sich um ein *Verbrauchergeschäft* handelt. Eigentumsverhältnisse an einzelnen Bestandteilen des Internet Of Things wurden vor dem Hintergrund der deutschen Rechtsordnung in einem Rechtsgutachten von *Wendehorst* erörtert und es wurde der Befund einer „strukturellen Erosion von Eigentum und Besitz" gestellt, die insbesondere den Verbraucher in eine ungünstigere Rechtsposition als die des Eigentümers bringt, weil das Ausmaß einzelner Rechte der Verbraucher in Bezug auf Bestandteile nicht gänzlich geklärt sei und zudem entstehe ein Abhängigkeitsverhältnis durch Bestandteile, die an Dienstleistungen oder eine Lizenzierung gebunden seien.[65] Diese Schlussfolgerungen können auch auf den österreichischen Rechtsraum übertragen werden. *Rabl* sieht Bestimmungen, die den Verbraucher schützen sollen als Hindernis für den Einsatz künstlicher Intelligenz, was schon durch das Beispiel der selbständig Waschmittel bestellenden Waschmaschine bei gleichzeitig bestehenden

Government Research, 282, ACM.

[62] In diesem Sinn auch *Hötzendorfer et al.* (2015) , die die Relevanz des Internet der Dinge für Smart Cities unterstreichen, siehe *Hötzendorfer, W., Meir Huber, M., Lemmel-Seedorf, R., Riegler, R., Schweighofer, E., Tjoa, S., Tschohl, C.* (2015), BEST AT Roadmap BEST AT Vertrauen rechtfertigen: sichere Systeme, S. 93. Verfügbar unter https://iktderzukunft.at/resources/pdf/best-at-roadmap.pdf

[63] *Rabl*, T., The Rise of the Machines – outsmarting the ABGB and everything else?, ecolex 2017, 611 (611).

[64] Siehe auch *Ganner, M./ Schmidt, H.* (2014), Ambient Assisted Living , iFamZ 2014, 118 (123).

[65] *Wendehorst*, C. (2016), Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, erstattet dem Sachverständigenrat für Verbraucherfragen Bundesministerium der Justiz und für Verbraucherschutz (BMJV), S.117 verfügbar unter http://www.svr-verbraucherfragen.de/wp-content/uploads/Wendehorst-Gutachten.pdf (abgerufen am 20.9.2017).

Verpflichtungen wie etwa zur Bereitstellung von Information vor Vertragsabschluss aufgezeigt werden könne; demgegenüber könnten Unternehmer im Rahmen der Privatautonomie die Nutzung von Algorithmen sehr wohl vereinbaren.[66]

Rechtsfragen in Zusammenhang mit autonomem Fahren betreffen nach *Hilgendorf* insbesondere das *Straßenverkehrs*recht, das Strafrecht, die Providerhaftung, das Datenschutzrecht und die zivilrechtliche Haftung für Schäden. Letztgenannte könnte vermehrt Hersteller treffen, weil das schädigende Verhalten des Systems diesem zugerechnet werden könnte. Mit Blick auf die strafrechtliche Haftung geht *Hilgendorf* davon aus, dass der tatsächliche Mehrwert des autonomen Fahrens für den Fahrer erst merklich erhöht würde, wenn von der Judikatur nicht strenge Sorgfaltspflichten in Bezug auf die Kontrolle des Systems (z.B. Reinigung von Sensoren) verlangt werden, wie dies in den Anfängen des Einsatzes eines solchen Systems der Fall sein dürfte. Auch Entscheidungen des Systems in Unfallsituationen (Abwägung Leben gegen Leben) werden thematisiert.[67] Wie dem deutschen Recht[68] ist auch der österreichischen Rechtsordnung eine Abwägung „Leben gegen Leben" fremd, daher stellt sich die Frage nicht, ob ein System gegen drei Leben und zu Gunsten der Rettung eines Lebens (oder umgekehrt) entscheiden darf. In der Praxis braucht es sicher die technische Implementierung von Regeln, nach welchen das autonom fahrende Auto reagieren wird. Mit *Hilgendorf*[69] kann festgehalten werden, die Frage, wie diese Programmierung bei gleichrangigen Rechtsgütern gelöst werden kann, ist noch ungelöst.

Es wurde – freilich noch nicht vor dem Hintergrund der DSGVO – vertreten, dass für die datenschutzrechtliche Zustimmung im Bereich von Systemen des *Ambiant Assisted Living* die Einsichts- und Urteilsfähigkeit (und nicht volle Geschäftsfähigkeit) Betroffener zu prüfen sei.[70] Diese Diskussion wurde inzwischen insofern eingeschränkt als der österreichische Gesetzgeber nun nach den Rahmenbedingungen der DSGVO lediglich das vollendete 14. Lebensjahr für eine zulässige Einwilligung fordert (siehe oben).

Zum Stand der *politischen Debatte* ist anzumerken, der Webseite des Parlaments ist ein 2015 eingebrachter Entschließungsantrag zu entnehmen, wonach ein Konzept für das digitale Österreich gefordert wird, in dessen Rahmen sich mit dem Thema Internet Of Things auseinandergesetzt werden soll und insbesondere auch gefordert wird, ein spezielles Ministerium für digitale Angelegenheiten

[66] *Rabl*, T., The Rise of the Machines – outsmarting the ABGB and everything else?, ecolex 2017, 611 (611-612).
[67] *Hilgendorf*, E., (2015), Automatisiertes Fahren und das Recht , ZVR 2015/240 (470-471).
[68] *Hilgendorf*, E. (2015), Automatisiertes Fahren und das Recht , ZVR 2015/240 (472).
[69] *Hilgendorf*, E., (2015), Automatisiertes Fahren und das Recht , ZVR 2015/240 (472).
[70] *Ganner*, M./ *Schmidt*, H. (2014), Ambient Assisted Living , iFamZ 2014, 118 (120).

einzurichten.[71] 2016 wurde auf den genannten Entschließungsantrag referenziert und auf das Regierungsprojekt Digital Roadmap sowie ein Grünbuch als Ergebnis einer vom Bundesratspräsidenten angestoßenen Enquete „Digitaler Wandel und Politik" verwiesen.[72] Ein Abgeordneter vertrat zu Internet of Things in derselben Sitzung die Meinung, es werde zu einem rasanten Anstieg digitaler Vernetzung kommen.[73] Die Webseite über die Digitalisierungsstrategie der Bundesregierung geht auch auf das Internet der Dinge ein und prognostiziert für das Jahr 2020 eine im Vergleich zu Menschen, die online sind, fast dreifache Anzahl an mit dem Internet verbundenen Geräten.[74] Es kann in diesem Rahmen keine Übersicht über den Stand der politischen Debatte gegeben werden. Die zuvor genannten Diskussionspunkte deuten jedoch darauf hin, dass einige Entscheidungsträger die Sensibilisierung für diesen Themenkreis vorantreiben. Als nächsten Schritt empfehlen *Hötzendorfer et al.* der Österreichischen Forschungsförderungsgesellschaft (FFG) die Förderung von Projekten, „welche die Analyse von Risiken durch vernetzte Objekte verbessern und sichere Lösungen entwickeln und testen".[75] Sehr maßgeblich ist jedenfalls auch die *rechtsethische Perspektive* in allfällige Überlegungen zur Weiterentwicklung oder Schaffung rechtlicher Möglichkeiten zur Nutzung von Internet Of Things oder künstlicher Intelligenz miteinzubeziehen.[76]

Ordnet man intelligente Messgeräte Internet Of Things zu, so kann als Beispiel für eine gesetzliche Maßnahme in diesem Bereich das Bundesgesetz, mit dem die Organisation auf dem Gebiet der Elektrizitätswirtschaft neu geregelt wird (Elektrizitätswirtschafts- und –organisationsgesetz 2010 – ElWOG

[71] Entschließungsantrag 1256/A(E) vom 07.07.2015 (XXV.GP); verfügbar unter https://www.parlament.gv.at/PAKT/VHG/XXV/A/A_01256/index.shtml (aufgerufen am 20.09.2017).

[72] Stenographisches Protokoll des NR, 146. Sitzung des NR, XXV. Gesetzgebungsperiode, 12. Oktober 2016, S. 168, verfügbar unter https://www.parlament.gv.at/PAKT/VHG/XXV/NRSITZ/NRSITZ_00146/fname_618301.pdf (aufgerufen am 20.09.2017). Das offenbar gemeinte Grünbuch ist unter http://www.besserentscheiden.at/digitaler-wandel-und-politik/ zugänglich (abgerufen am 20.09.2017).

[73] Stenographisches Protokoll des NR, 146. Sitzung des NR, XXV. Gesetzgebungsperiode, 12. Oktober 2016, S. 169, verfügbar unter https://www.parlament.gv.at/PAKT/VHG/XXV/NRSITZ/NRSITZ_00146/fname_618301.pdf (aufgerufen am 20.09.2017).

[74] Bundeskanzleramt und Bundesministerium für Wissenschaft, Forschung und Wirtschaft (Hrsg.) https://www.digitalroadmap.gv.at/ (abgerufen am 20.09.2017).

[75] *Hötzendorfer, W., Meir Huber, M., Lemmel-Seedorf, R., Riegler, R., Schweighofer, E., Tjoa, S., Tschohl, C.* (2015), BEST AT Roadmap BEST AT Vertrauen rechtfertigen: sichere Systeme, S. 94. Verfügbar unter https://iktderzukunft.at/resources/pdf/best-at-roadmap.pdf

[76] Auch das im Auftrag des Präsidenten des Bundesrates erstellte Grünbuch „Digitale Courage" geht auf ethische Aspekte ein, siehe Parlamentsdirektion (Hrsg.) (2016), Grünbuch Digitale Courage, Wien; verfügbar unter https://www.parlament.gv.at/ZUSD/PDF/Gruenbuch_Digitale_Courage_Republik_Oesterreich_Bundesrat.pdf (abgerufen am 20.09.2017).

2010), BGBl I Nr. 110/2010 idF BGBl I Nr. 108/2017, genannt werden, worin die Verwendung *intelligenter Messgeräte* geregelt ist.[77]

Frage 4.4.

Vor der Anpassung des DSG im Hinblick auf die DSGVO durch das Datenschutz-Anpassungsgesetz 2018, welche Änderungen nach § 70 Abs 1 DSG mit 25. Mai 2018 in Kraft treten wird, regelt aktuell § 27 DSG 2000 das Recht auf Richtigstellung oder Löschung. Nach *Kamann/Braun*[78] behandelt Art 17 Abs 1 DSGVO das „klassische Löschungsrecht", Art 17 Abs 2 DSGVO hingegen das „Recht auf Vergessenwerden" im engeren Sinn.[79] Herbst weist darauf hin, dass Suchmaschinenbetreiber gem Art 17 Abs 2 DSGVO zu informieren sein werden und die „Google Spain"-Entscheidung Hinweise für die Beurteilung der Frage bietet, ob Suchmaschinenbetreiber den Ergebnislink zu löschen haben werden.[80] Nach *Hasenauer* ist die Tätigkeit einer Suchmaschine eine „Verwendung von Daten" iSd § 4 Z 8 DSG 2000, das heißt, das DSG 2000 steht im Einklang mit der bejahenden Beantwortung der Frage durch den EuGH, ob die Tätigkeit der Suchmaschine eine Datenverarbeitung darstellt.[81] Zur Frage, ob der Betreiber der Suchmaschine ein für die Verarbeitung Verantwortlicher ist, wurden im Schrifttum in Österreich unterschiedliche Meinungen vertreten.[82]

Die Datenschutzbehörde wurde mit dem Fall konfrontiert, dass Insolvenzdaten auf einer – im Gegensatz zur Ediktsdatei – für Suchmaschinen nicht gesperrten Seite veröffentlicht wurden.

Beschwerdegegnerin war die Wirtschaftskammer Oberösterreich, die Insolvenzdaten über den Beschwerdeführer offenbar im elektronischen Archiv der OÖ Wirtschaft-Kammernachrichten in einer Art speicherte, die bei der Suche nach dem Namen des Beschwerdeführers zum Auffinden dieser Informationen mittels

[77] Siehe *Knyrim, R./ Trieb, G.*, Smart Metering NEU – die Änderungen durch die ElWOG-Novelle 2013 (2013), ecolex 2013, 1123.

[78] *Kamann, H.-G., Braun, M. in Ehmann, E. und Selmayr, M.* (Hrsg.), DS-GVO Datenschutz-Grundverordnung Kommentar, C.H.BECK LexisNexis, 2017, Art 17, Rz 3.

[79] Zur Verankerung des Rechts auf Vergessenwerden in Abs 2 vgl. auch Feiler, L./Forgó, N., (2017), EU-DSGVO EU-Datenschutz-Grundverordnung Kurzkommentar, Verlag Österreich, Wien, Art 17, Anm 1.

[80] *Herbst, T. in Kühling, J. und Buchner,* B., (2017), DS-GVO Datenschutz-Grundverordnung Kommentar, C.H.BECK, Art 17, Rz 69.

[81] *Hasenauer*, S., (2014), Das Recht auf Löschung personenbezogener Daten. Das "Google-Spain und Google"-Urteil des EuGH vom 13. 5. 2014 (FN 1, Jahrbuch Datenschutzrecht 2016, 99 (111).

[82] Bejahend und somit dem EuGH zustimmend z.B. Hasenauer, S., (2014), Das Recht auf Löschung personenbezogener Daten. Das "Google-Spain und Google"-Urteil des EuGH vom 13. 5. 2014 (FN 1, Jahrbuch Datenschutzrecht 2016, 99 (113); anderer Ansicht z.B. Wolfgang Zankl, EuGH: "Recht auf Vergessenwerden", ecolex 2014, 676, der auf die Konzeption einer Suchmaschine als Vermittler im ECG, auf den bestehenden zivilrechtlichen Löschungsanspruch bei Unrichtigkeit sowie auf Schwierigkeiten bei der Durchsetzung eines Löschungsanspruchs im weltweiten Internet hinweist.

Suchmaschine führten. Im Zeitpunkt der Entscheidung durch die Datenschutzbehörde bestand kein Rechtsschutzbedürfnis mehr, weil die Informationen über Suchmaschinen nicht mehr auffindbar waren.[83]

Für die Geltendmachung des subjektiven Rechts auf Geheimhaltung bzw. Löschung von Daten gegenüber privaten Rechtsträgern ist der Zivilrechtsweg vorgesehen.[84] Der OGH behandelte in zwei Entscheidungen (Autocomplete OGH vom 30.03.2016, 6Ob26/16s sowie Autocomplete II OGH vom 22.12.2016, 6Ob241/16h) Anträge im Zusammenhang mit Funktionen der automatischen Vervollständigung von Suchmaschinen. Dabei wurde die Entfernung von Links Dritter zwar nicht beurteilt, jedoch wurde auf die Interessenabwägung eingegangen.

In Autocomplete II wurde von der Verknüpfung des früheren Namens der Klägerin mit einem niederländischen Ort und der niederländischen Bezeichnung für Zahnarzt mit dem aktuellen Namen der Klägerin und dem Begriff Zahnärztin sowie davon ausgegangen, dass die Berichterstattung über eine flüchtende Zahnärztin nicht mit dem aktuellen Namen der Klägerin verbunden werden konnte. Eine Beeinträchtigung der Persönlichkeitsrechte der Klägerin wurde nicht erkannt. In Bezug auf die Abwägung der Interessen wurde auf die vorangegangene Entscheidung Autocomplete mit derselben Klägerin verwiesen. Aus dieser Entscheidung Autocomplete geht hervor, dass der Klägerin von der niederländischen Standesaufsichtsbehörde zwei Verweise erteilt wurden. Nach erfolglosen Ersuchen auf Eintragung in die britische Liste der Zahnärzte unter ihren früheren Namen, wurde diesem Ersuchen nachgekommen als die Klägerin ihre Vor- und Nachnamen geändert hatte. Die Streichung von dieser Liste erfolgte durch Disziplinarentscheidung. Die Suchmaschine kombinierte in der automatischen Vervollständigung insbesondere die früheren Namen mit den neuen Namen der Klägerin. Der OGH hatte sohin zu beurteilen, ob die Vervollständigung mit dem geänderten Namen durch die Autocomplete-Funktion zulässig war. Die Ansicht des Rekursgerichts wurde wie folgt zusammengefasst: „Das in der Namensanonymität konkretisierte Persönlichkeitsrecht und der Schutz der Privatsphäre seien gegen das Informationsinteresse abzuwägen. Diese Interessenabwägung schlage hier insbesondere aufgrund der Disziplinarentscheidung der britischen Standesaufsichtsbehörde zugunsten der Öffentlichkeit aus."[85]

Der OGH schloss sich der Ansicht des deutschen BGH an, der AutoComplete-Vorschläge (anders als Suchergebnisse) als eigene Inhalte des Such-

[83] Datenschutzkommission vom 21.01.2009, K121.378/0003-DSK/2009.
[84] Datenschutkommission vom 18.05.2004, K211.496/0003-DSK/2004.
[85] OGH vom 30.03.2016, 6Ob26/16s.

maschinenanbieters qualifizierte.[86] Die zentrale Frage war, „ob die Klägerin einen Anspruch hat, dass ihr früherer bürgerlicher Name (...) geheim gehalten beziehungsweise nicht in Verbindung mit ihrem aktuellen Namen gebracht wird"[87], relevante Rechtsgrundlage war § 16 ABGB. „Hat der Betroffene nicht zugestimmt und besteht weder ein gesetzliches Verbot noch eine ausdrückliche gesetzliche Ermächtigung, hängt die Frage der Rechtswidrigkeit der Namensnennung deshalb von einer vorzunehmenden Interessenabwägung ab (RIS-Justiz RS0009319 [T3], RS0008998)(...) Ist die Namensnennung nicht gesetzlich verboten und hat der Namensträger einen sachlichen Anlass zur Nennung seines Namens gegeben, dann wiegt das *Informationsbedürfnis der Öffentlichkeit* hingegen regelmäßig schwerer als der *Schutz der Privatsphäre* (RIS-Justiz RS0008998 [T8], RS0009003 [T3])."[88] Der OGH entschied, die Nennung des früheren Namens der Klägerin begründe keine Verletzung der Persönlichkeitsrechte oder Beeinträchtigung der Privatsphäre. „Bei einer Interessenabwägung ist zu berücksichtigen, dass die Klägerin zu 4 Ob 155/09m Opfer eines Verbrechens geworden war, während im vorliegenden Fall die Klägerin bei der britischen Standesbehörde evidentermaßen vorsätzlich falsche Angaben gemacht hatte."[89]

In OGH vom 28.11.2013, 6Ob165/13b, setzt sich der OGH mit der unbeabsichtigten Aufnahme von Daten über Gerichtsverfahren in den Google Cache auseinander und kommt zu dem Schluss dass die Daten – entgegen des Vorbringens des Bundes – nicht allgemein verfügbar waren, was gemäß § 1 DSG 2000 zu mangelndem schutzwürdigen Geheimhaltungsinteresse und damit zum Nichtvorliegen eines Grundrechtseingriffs geführt hätte, sondern sehr wohl ein Grundrechtseingriff stattfand. Besonders die Ansicht von *Lehner/Lachmayer*, es liege bei der betroffenen Person, zu entscheiden, welche Information sie als zu ihrer Privatsphäre gehörig bewerte und wie die Person sich in Bezug auf diese Information verhalte[90], erscheint maßgeblich für zukünftige Bewertungen.

Nichtsdestotrotz ist mit *Hasenauer* festzuhalten, „Eine offene Frage auf europäischer und nationaler Ebene betrifft die Interessenabwägung auf grundrechtlicher Ebene, auf die Gerichte wohl in zukünftigen Entscheidungen auch näher eingehen werden."[91]

[86] OGH vom 30.03.2016, 6Ob26/16s, Rechtliche Beurteilung, 3.1. mit umfangreichen Nachweisen und 3.2.

[87] OGH vom 30.03.2016, 6Ob26/16s, Rechtliche Beurteilung, 4.

[88] OGH vom 30.03.2016, 6Ob26/16s, Rechtliche Beurteilung, 4.1.

[89] OGH vom 30.03.2016, 6Ob26/16s, Rechtliche Beurteilung, 4.3.

[90] OGH vom 30.03.2016, 6Ob26/16s, Rechtliche Beurteilung, 3.2. mit Verweis auf *Lehner/Lachmayer*, Datenschutz im Verfassungsrecht, in Bauer/Reimer, Handbuch Datenschutzrecht (2009), 98 f u.a.

[91] *Hasenauer*, S., (2014), Das Recht auf Löschung personenbezogener Daten. Das "Google-Spain und Google"-Urteil des EuGH vom 13. 5. 2014 (FN 1, Jahrbuch Datenschutzrecht 2016, 99 (130-131).

BELGIUM

Jean-Benoît Hubin[*] • Hervé Jacquemin[**] • Michael Lognoul[***]
Christian Hocepied[****] • Michael Lognoul[*****]
Elise Degrave[******] • Antoine Delforge[*******]
Thomas Tombal[********] • Noémie Gillard[*********] • Quentin Van Enis

1. Marché Intérieur et commerce électronique: Internet et commerce électronique

1.1. Commerce électronique, responsabilité des intermédiaires de l'Internet: questions spécifiques

Question 1.1.1.

Suite à l'émergence du web 2.0, les juridictions belges ont été confrontées à la nécessité d'interpréter les concepts de la directive 2000/31, et en particulier la notion d'hébergeur, au regard de l'évolution de l'internet. Elles ont ainsi dû qualifier

* Assistant à l'UNamur (CRIDS - Centre de Recherche, Information, Droit et Société www.crids.eu) et avocat au barreau de Namur. Contributeur Q1.
** Chargé de cours à l'UNamur (CRIDS) et avocat au barreau de Bruxelles. Contributeur Q1.
*** Assistant à l'UNamur (CRIDS). Contributeur Q2.
**** Chercheur au CRIDS. Contributeur Q3.
***** Assistant à l'UNamur (CRIDS). Contributeur Q3.
****** Chargée de cours à l'UNamur (CRIDS). Contributrice Q4.1.
******* Chercheur au CRIDS. Contributeur Q4.2.
******** Chercheur au CRIDS. Contributeur Q4.3.
********* Chercheuse au CRIDS. Contributrice Q4.3.
********** Chargé de cours à l'UNamur (CRIDS), chargé de cours invité à l'UCL et avocat au barreau de Bruxelles). Contributeur Q4.4.

l'activité d'un moteur de recherche, d'un prestataire de service de forum de discussion ou d'une place de marché en ligne au regard du concept d'hébergeur:

- Dans un arrêt du 3 février 2004, la Cour de cassation de Belgique a posé le principe selon lequel l'exonération de responsabilité en faveur des prestataires intermédiaires de l'internet s'applique «*dans la mesure où leur activité revêt un caractère purement technique, automatique et passif, ce qui implique que l'intermédiaire ne connaît pas et n'exerce pas de contrôle sur l'information qui est transmise ou stockée*»[1].
- Avant que la Cour de cassation ait pris position, la Cour d'appel d'Anvers avait estimé, à juste titre, que l'exploitant d'un **site web fournissant des hyperliens** qui dirigeaient le trafic vers des sites web à contenus pédopornographiques, ne pouvait être assimilé à un prestataire intermédiaire, dès lors qu'il faisait preuve d'un engagement en assemblant ces hyperliens de manière consciente[2].
- S'agissant de l'activité d'un *forum de discussion*, la Cour d'appel de Bruxelles a refusé la qualité d'hébergeur au modérateur d'un forum, proposant une analyse technique du concept d'hébergeur et relevant, par ailleurs, que la personne poursuivie en qualité de modérateur s'était réservée un droit de contrôle (sous la forme d'un droit de retrait) sur les propos échangés sur le forum de discussion[3].

  Appliquant de manière plus souple les principes de la directive 2000/31, le tribunal de première instance d'Anvers a par contre considéré que les gestionnaires d'un forum de discussion non commercial ne pouvaient être tenus pour responsables des informations diffusées sur le forum, dès lors qu'ils avaient adopté une réaction quasi immédiate pour rendre ces informations illisibles[4].

  Suite à l'arrêt *Delfi* de la Cour européenne des droits de l'homme[5], la jurisprudence belge sera confrontée à la nécessité de résoudre les tensions pouvant apparaître entre cette jurisprudence se fondant sur les articles 8 et 10 de la Convention européenne des droits de l'homme, et la jurisprudence de la Cour de justice de l'Union européenne. La position adoptée par la Cour européenne des droits de l'homme dans l'arrêt *Delfi* semble, en effet, sous certains aspects, susceptible d'entrer en conflit avec le concept de prestataire intermédiaire, tel qu'interprété par la Cour de cassation et par la Cour de justice.

[1] Cass., 3 février 2004, *Pas.*, 2004, p. 200.
[2] Anvers, 7 octobre 2003, *A&M*, 2004, p. 164.
[3] Bruxelles, 25 novembre 2009, *R.D.T.I.*, 2010, p. 102.
[4] Civ. Anvers, 3 décembre 2009, *A&M*, 2010, p. 560.
[5] C.E.D.H., 16 juin 2015, Req n° 64569/09, *Delfi c. Estonie*.

- Saisi de la qualification de l'activité d'une plateforme proposant un service de *place de marché en ligne*, le tribunal de commerce de Bruxelles a proposé une interprétation évolutive du concept de prestataire intermédiaire, tenant compte du développement des activités proposées sur internet. Il a d'abord relevé que «*si, à l'origine du commerce électronique, l'on pouvait concevoir que les services visés à la section 4 de la directive seraient fournis par des opérateurs spécialisés ne fournissant que tel ou tel service, il est vite apparu que les fournisseurs de ces services proposaient en outre d'autres services et assumaient d'autres activités conduisant à ce que leur site internet présente une nature composite*». Il a ensuite appelé à distinguer les activités exercées par un prestataire de service et à déterminer, parmi celles-ci, les activités pouvant bénéficier de l'exemption instaurée par la directive 2000/31, quelles que soient les autres activités exercées par ailleurs par ce prestataire. Il a conclu qu'en l'espèce les annonces de ventes postées sur la place de marché en ligne faisaient l'objet d'un service d'hébergement dans le chef de la plateforme, justifiant l'application du régime d'exonération de responsabilité[6].
- Enfin, la Cour d'appel de Bruxelles a jugé «*que les* ***moteurs de recherche*** *ne bénéficient pas du régime juridique spécifique à la catégorie des intermédiaires techniques*», après avoir rappelé «*que le choix du législateur européen était de ne pas inclure les moteurs de recherche dans les prestataires de services intermédiaires bénéficiant d'une exonération de responsabilité* »[7].

Dans cette même affaire, la Cour d'appel de Bruxelles a rappelé que le régime d'exonération de responsabilité applicable au prestataire d'un service 'en cache' s'appliquait à une prestation de stockage destinée «*exclusivement à l'exécution de la transmission sur le réseau de communication et pour autant que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission*». Selon la Cour d'appel, si le service 'en cache' proposé par le prestataire poursuit d'autres fonctions, et qu'il reste disponible pendant une durée excédant l'exigence de transitivité éphémère, il ne peut être assimilé à une activité liée à la transmission des contenus sur les réseaux, exonérée en vertu de l'article 13 de la directive 2000/31.

Question 1.1.2.

Dans son arrêt L'Oréal c/eBay, la Cour de justice a jugé que l'exonération de responsabilité bénéficiant aux prestataires intermédiaires ne pouvait s'appliquer «*lorsque le prestataire du service, au lieu de se limiter à une fourniture neutre de celui-ci au moyen d'un traitement purement technique et automatique des données fournies par*

[6] Comm. Bruxelles, 31 juillet 2008, *R.D.T.I.*, 2008, p. 521.

[7] Bruxelles, 5 mai 2011, *R.D.T.I.*, 2011, n° 44, p. 35.

ses clients, joue un rôle actif de nature à lui confier une connaissance ou un contrôle de ces données»[8]. La Cour de justice a ainsi fait du critère de neutralité une condition indispensable de l'application du régime d'exonération. Ceci rejoint les principes dégagés par la jurisprudence belge.

Dans l'hypothèse d'un service de place de marché en ligne, la Cour de justice a considéré quele simple fait de stocker des offres de vente moyennant rémunération et de donner des informations d'ordre général ne faisait pas perdre ce caractère neutre au prestataire de service. Par contre, selon la Cour de justice, le fait de prêter assistance en vue d'optimiser la présentation des offres confère un caractère actif à l'intervention du prestataire de service de place de marché en ligne, susceptible de le priver du bénéfice de l'exonération de responsabilité prévue par la directive 2000/31.

L'analyse proposée par la Cour de justice nous paraît devoir être complétée par celle fournie par le Tribunal de commerce de Bruxelles dans son jugement du 31 juillet 2008[9], dans laquelle le Tribunal de commerce avait souligné qu'il y avait lieu, avant d'analyser l'activité du prestataire de services à la lumière des principes fixés par la directive 2000/31, de distinguer les différents services offerts et de déterminer, pour chacun de ces services, si ceux-ci conduisent le prestataire à jouer un rôle actif ou non.

Question 1.1.3.

Le régime de notification et de retrait apporte, incontestablement, un remède efficace aux publications abusives dans le contexte de l'internet. Il garantit aux personnes préjudiciées d'obtenir une solution rapide au problème qu'elles rencontrent. Ce système n'est toutefois pas à l'abri de demandes de retrait abusives, pouvant porter atteinte au droit à la liberté d'expression. C'est pourquoi, à défaut de faire l'objet d'un contrôle judiciaire adéquat, ce régime peut confronter le prestataire intermédiaire à certaines difficultés, en ce qu'il pourrait l'obliger à arbitrer, dans certaines situations, un conflit entre l'auteur de la demande de retrait et l'auteur de la publication initiale, se prévalant de son droit à la liberté d'expression. Dans cette hypothèse, le prestataire intermédiaire se verra placé dans une position particulièrement inconfortable, étant susceptible, en fonction de la décision qu'il prend, d'engager sa responsabilité à l'égard de l'une ou l'autre des parties.

Une solution alternative pourrait se dégager progressivement. Elle consisterait à donner à la personne lésée par une publication en ligne le droit de solliciter des cours et tribunaux, dans le cadre d'une procédure unilatérale, une injonction

[8] § 113.

[9] Cfr. Question n° 1.1.1. ci-dessus.

visant à faire cesser, à titre provisoire à tout le moins, la diffusion de l'information litigieuse. La mise en place de ce type de procédure permettrait à la personne préjudiciée par la publication d'obtenir une solution rapide, sans préjudice d'un débat judiciaire ultérieur donnant le droit au prestataire intermédiaire, et le cas échéant à l'auteur de la publication, de faire valoir leurs droits, notamment leur droit à la liberté d'expression. Un tel système peut être assimilé à une forme de judiciarisation de la procédure de notification et retrait.

Question 1.1.4.

Les juridictions belges ont principalement été confrontées à la difficulté de définir la portée des injonctions pouvant être prononcées à l'égard d'un prestataire intermédiaire, afin de tenir compte des principes dégagés par la Cour de justice dans sa jurisprudence visant à préserver un équilibre avec différents droits fondamentaux.

S'agissant d'une mesure de blocage, la Cour de cassation a jugé que «*l'ordre adressé à un fournisseur d'accès à internet de bloquer par tous les moyens techniques possibles l'accès au contenu hébergé par un serveur associé à un nom de domaine principal déterminé en bloquant à tout le moins tous les noms de domaine qui renvoient à ce serveur associé au nom de domaine principal déterminé, avec de surcroît la spécification du procédé technique devant être employé, n'implique pas l'obligation de surveillance visée par l'article 15.1 de la directive*»[10].

Pour ce qui est des injonctions conduisant au retrait de certaines publications, la Cour d'appel d'Anvers a rappelé que celles-ci devaient présenter une portée limitée, jugeant que la mesure prise par le juge ne pouvait en aucun cas avoir pour conséquence que la publication, la distribution ou la diffusion de l'expression d'une opinion soit empêchée ou soumise à condition[11].

Les juridictions belges sont par ailleurs confrontées à la difficulté de veiller à l'effectivité des injonctions qu'elles prononcent. Les auteurs d'infractions en ligne développent, en effet, régulièrement des stratagèmes leur permettant de contourner l'effet des injonctions prononcées.

Enfin, la Cour de cassation a tranché la controverse de savoir si la personne préjudiciée par une publication sur internet pouvait puiser dans la législation existante un droit subjectif lui permettant d'exiger du prestataire intermédiaire que lui soit communiquée l'identité de la personne à l'origine de la publication litigieuse. La Cour de cassation s'est opposée à une telle mesure, considérant que «*cette disposition ne confère pas à une personne qui soutient être victime de propos calomnieux ou diffamatoires publiés sur le site d'un prestataire de services le droit subjectif*

[10] Cass., 22 octobre 2013, *Pas.*, 2013, p. 2005.

[11] Anvers, 20 décembre 2006, *A&M*, 2008, p. 133.

d'obtenir d'une juridiction de l'ordre judiciaire qu'elle ordonne à ce prestataire de lui communiquer toutes les informations dont il dispose sur les prétendus auteurs d'infractions aux fins de poursuivre une action civile en réparation»[12].

1.2. Protection des consommateurs en matière d'Internet et de commerce électronique, d'achats sur internet et de droits contractuels ; protection des consommateurs et résolution de litiges

Question 1.2.1.

La directive 1999/44/CE du Parlement européen et du Conseil, du 25 mai 1999, sur certains aspects de la vente et des garanties des biens de consommation[13] a été transposée en droit belge par la loi du 1er septembre 2004 relative à la protection des consommateurs en cas de vente de biens de consommation[14]. Plus précisément, de nouvelles dispositions ont été introduites dans le Code civil (art. 1649*bis* et s.). Dans le contexte général de l'économie numérique, la question se pose de savoir, d'une part, (i) si ces dispositions s'appliquent aux contrats conclus à distance et par voie électronique et, dans l'affirmative, si les consommateurs s'en prévalent à l'occasion de recours contre des entreprises, d'autre part, (ii) s'il est également permis d'invoquer les mesures de protection en matière de contenus numériques (au sens de l'art. 2, 11°, de la directive 2011/83/UE sur les droits des consommateurs).

L'application des articles 1649*bis* et suivants du Code civil n'est pas conditionnée par le mode de conclusion du contrat (en présence physique des parties, à distance, en ligne, hors établissement, etc.). Dès lors qu'il y a vente d'un bien de consommation, d'un vendeur à un consommateur, le régime spécifique tiré de la directive 1999/44/CE s'applique, en ce compris lorsque le contrat est conclu à distance et par voie électronique. On trouve d'ailleurs de la jurisprudence publiée dans cette dernière hypothèse même s'il faut reconnaître que les décisions restent assez rares[15]. Ce n'est pas une surprise: tenant compte de l'enjeu du litige, comparé au coût de la procédure, sa longueur, et l'incertitude de l'issue, les consommateurs hésiteront généralement à porter le litige devant les cours et tribunaux. Par contre, les procédures de règlement extrajudiciaire des litiges de consommation, telles que visées par le livre XVI du Code de droit économ-

[12] Cass., 16 juin 2011, *Pas.*, 2011, p. 1672.

[13] *J.O.*, L 171 du 7 juillet 1999.

[14] *M.B.*, 21 septembre 2004.

[15] Voy. not. Liège 25 mars 2011, *R.D.T.I.*, 2012/46, p. 67, note J.-F. Henrotte (le litige portait sur la vente d'une voiture à travers la plateforme de commerce électronique eBay, qui était tombée en panne après avoir parcouru ... 2 kilomètres); Prés. Comm. Nivelles, 29 février 2012, *Ann. Prat. Comm.*, 2012, p. 63 (litige entre entreprises dans le cadre d'une action en cessation commerciale où la garantie des biens de consommation est évoquée à la marge).

ique, connaissent un succès croissant. En témoigne le Rapport annuel 2016 du Service de médiation pour les consommateurs[16], publié en septembre 2017 et qui montre que la majorité des plaintes concernent des problèmes de garanties (839 plaintes), les troisième et quatrième positions du tableau étant par ailleurs occupées par les produits/services défectueux (327 plaintes) et la non-conformité (325 plaintes). Les mesures établies par les articles 1649*bis* et suivants du Code civil sont par conséquent capitales pour assurer un niveau élevé de protection du consommateur.

Plus discutable est l'application des articles 1649*bis* et suivants du Code civil aux contenus numériques (applications, logiciels, films visionnés en streaming, contenus partagés sur les réseaux sociaux, etc.)[17]: conformément à l'article 1649*bis*, § 2, 3°, le bien de consommation est «tout objet mobilier corporel, sauf [...]». Les discussions doctrinales relatives à la qualification des logiciels, notamment dans le contexte des ventes de biens de consommation, montrent à quel point il est délicat de procéder à l'exercice de qualification. Des auteurs jugent ainsi que les logiciels sont des biens corporels dans tous les cas[18], quand d'autres se montrent plus nuancés et distinguent suivant que le logiciel est exécuté en ligne (auquel cas il est incorporel) ou enregistré sur un support physique (auquel cas, il est corporel)[19].

[16] Disponible sur https://www.mediationconsommateur.be/sites/default/files/content/download/files/cod-jaarverslag_2016-fr-def-hr.pdf.

[17] De manière générale, voy. M.B.M. Loos, N. Helberger, L. Guibault, C. Mak, L. Pessers, J.K. Cseres, B. van der Sloot et R. Tigner, *Comparative analysis, Law and Economics analysis, assessment and recommendations for possible future rules on digital content contracts,* étude de l'Université d'Amsterdam, 2011; U. Stenzel, M. G. S. Lima et J.J. Downes, *Study on Digital Content Products in the EU,* IBF International Consulting for the European Commission, 2012, 86 p.; N. Helberger, M.B.M. Loos, L. Guibault, C. Mak et L. Pessers, «Digital Content Contracts for Consumers», *J. Consum. Policy,* 2013/36, pp. 37-57; J. Jacquemin, «La protection du consommateur de contenus numériques», *D.C.C.R.,* 2015/108-109, pp. 5 et s.

[18] M. Tenreiro et S. Gómez, «La directive 1999/44/CE sur certains aspects de la vente et des garanties de biens de consommation», *R.E.D.C.,* 2000, p. 12: «un bien électronique (qui consiste en une quantité de données et qui occupe un espace physique, par exemple dans la mémoire d'un ordinateur), doit être considéré comme bien corporel et doit donc être soumis au champ d'application de la directive. Le fait qu'il soit fourni au consommateur dans un support matériel ou à travers un réseau doit être sans importance».

[19] L. Serrano, «Article 1er. Champ d'application et définitions», M.C. Bianca, S. Grundmann et S. Stijns (dir.), *La directive communautaire sur la vente – Commentaire,* Bruxelles, Bruylant, Paris, L.G.D.J., 2004, p. 130. Voy. aussi Ch. Biquet-Mathieu, «La garantie des biens de consommation – Présentation générale», *La nouvelle garantie des biens de consommation et son environnement légal*, Bruxelles, La Charte, 2005, pp. 64-65 (qui considère que les logiciels ou les enregistrements audio/vidéo vendus sur un support physique sont des biens corporels, tout en admettant que la question est controversée s'agissant des téléchargements).

A la lumière de l'interprétation des dispositions de la directive 2011/83/UE sur les droits des consommateurs, c'est ce dernier point de vue qui paraît confirmé[20](ce qui, d'après nous, est contestable) : suivant la directive, il faut en effet distinguer les contenus numériques fournis sur un support matériel (et qui constituent des «biens», au sens de la directive) et les contenus numériques qui ne sont pas fournis sur un support matériel (et qui répondent normalement à la définition de «service», au sens de la directive). Cette manière de faire crée d'après nous des différences de traitement potentiellement contraires au principe d'égalité et de non-discrimination (art. 10-11 Const.). Un régime cohérent devrait ainsi être appliqué à tout type de contenu numérique. Il faut en effet éviter de traiter de manière différente un même contenu numérique, en fonction de la manière dont il est transmis (sur un support matériel ou pas) et du prix éventuellement payé par le consommateur. On se réjouit dès lors de la proposition de directive concernant certains aspects des contrats de fourniture de contenu numérique[21], qui complète le cadre normatif applicable aux contenus numériques (en ajoutant des mesures de protection, notamment dans le domaine de la conformité et de la garantie).

Question 1.2.2.

La directive proposée concernant certains aspects des contrats de fourniture de contenu numérique (COM(2015)634) prévoit-elle des règles appropriées permettant la mise en place d'un véritable marché unique numérique?

La fourniture de contenus numériques aux consommateurs fait l'objet de mesures spécifiques de protection conformément à la directive 2011/83/UE sur les droits des consommateurs (elles sont transposées dans les livres VI et XIV du Code de droit économique). Elles consistent principalement en l'octroi d'informations spécifiques[22] et l'aménagement de l'exercice du droit de rétractation[23] (conduisant généralement à priver le consommateur de l'exercice dudit droit dans l'hypothèse de contenus numériques).

Pour les contrats portant sur la fourniture de contenus numériques (en tout cas s'ils ne sont pas fournis sur un support matériel – cf. *supra*, question 1.2.1.), le

[20] Le considérant n° 19 de la directive sur les droits des consommateurs indique la signification à donner au contenu numérique «au sens de la directive». On ne peut donc exclure qu'un même terme reçoive une acception différente suivant une autre directive. Par souci de cohérence, une interprétation uniforme devrait normalement être défendue, dans la mesure du possible.

[21] COM(2015) 634 final.

[22] Art. 5 (1), g) et h), et art. 6 (1), r) et s), de la directive 2011/83/UE.

[23] Voy. en particulier l'art. 16, m), de la directive 2011/83/UE: pas de droit de rétractation pour «la fourniture d'un contenu numérique non fourni sur un support matériel si l'exécution a commencé avec l'accord préalable exprès du consommateur, lequel a également reconnu qu'il perdra ainsi son droit de rétractation».

régime de protection en matière de garantie des biens de consommation n'est pas applicable.

On observe pourtant que, dans l'hypothèse de contenus numériques, la faiblesse du consommateur aurait justifié l'adoption de mesures de protection complémentaires. C'est en effet l'objet du contrat qui explique la faiblesse du consommateur: le contenu numérique se caractérise par des éléments de nature technique (et qui tiennent notamment à ses fonctionnalités, son interopérabilité avec d'autres matériels ou logiciels ou aux restrictions géographiques éventuelles), que le consommateur moyen ne maîtrise pas nécessairement. De nombreux consommateurs peuvent aussi être surpris de l'exigence de paiement d'un prix en cours d'exécution du contrat (pour progresser dans un jeu sur appareil mobile, par exemple, le téléchargement de l'application de base étant gratuit). Par ailleurs, il n'est pas rare que des données à caractère personnel soient traitées à travers les applications mises à sa disposition ou que des droits de propriété intellectuelle lui soient octroyés. A cet égard, le consommateur souffrira généralement d'un manque d'information sur les éléments de droit liés à ces considérations, lorsqu'il ignore les traitements réalisés avec ses données ou qu'il ne connaît pas l'étendue de son droit d'utilisation sur le logiciel téléchargé. On ajoute que s'agissant de contrats d'adhésion, la marge de négociation du consommateur est très réduite, voire inexistante; tout au plus peut-il se borner à adhérer au contrat standardisé qui lui est proposé (au risque d'accepter des conditions déséquilibrées).

L'adoption de règles complémentaires en vue de protéger le consommateur de contenus numériques est donc souhaitable. Aussi la proposition de directive concernant certains aspects des contrats de fourniture de contenu numérique doit-elle être approuvée dans son principe. A la différence de la directive 2011/83/UE sur les droits des consommateurs, qui mobilise principalement des mesures de protection contemporaines à la formation du contrat, la proposition encadre également les difficultés susceptibles de se présenter en cours d'exécution de celui-ci (avec les problèmes de conformité, la responsabilité éventuelle du prestataire, la modification du contenu, la dissolution du contrat, la récupération des contenus, etc.).

Si l'initiative de la Commission doit être approuvée en ce qu'elle renforce sensiblement la protection des consommateurs de contenus numériques, plusieurs critiques peuvent néanmoins être pointées. L'acception de la notion de «contenu numérique» et le champ d'application de la proposition sont en effet discutables à certains égards, spécialement quant aux liens qui sont faits avec les données personnelles fournies en contrepartie du contenu (cf. art. 3). L'articulation avec d'autres dispositions en vigueur pourrait également être source de difficultés: on songe au Règlement général de protection des données (concernant le droit à la portabilité des données, à articuler avec l'article 16 (4) (b) de la proposition

de directive) ou à la directive sur les droits des consommateurs (et sa distinction entre les contenus numériques fournis sur un support matériel ou pas). On peut également regretter que des mesures spécifiques ne soient pas prises au bénéfice des mineurs, pourtant grands consommateurs de contenus numériques.

Le texte déposé par la Commission est actuellement en discussion et il fera probablement l'objet d'amendements. Aussi faut-il espérer qu'ils iront vers une plus grande clarté des règles applicables.

Question 1.2.3.

Contrairement à ce que l'intitulé de la proposition de directive concernant certains aspects des contrats de vente en ligne aurait pu laisser croire, elle n'introduit pas de mécanismes de protection justifiés exclusivement par la faiblesse du consommateur qui s'engage à distance (avec un renforcement des obligations d'information ou l'octroi d'un droit de rétractation). Ces règles se trouvent déjà dans la directive 2011/83/UE sur les droits des consommateurs et la directive 2000/31/CE sur le commerce électronique.

A l'analyse, les mesures introduites par la proposition de directive concernent uniquement la conformité des biens et les modalités de dédommagement en cas de non-conformité. Ces questions étaient déjà réglées par la directive 1999/44/CE sur certains aspects de la vente et des garanties des biens de consommation. Il s'agissait toutefois d'une directive d'harmonisation minimale: des différences existent donc entre les législations des Etats membres, avec les difficultés qui en résultent pour les prestataires qui souhaitent se lancer dans le commerce électronique transfrontière.

La proposition s'applique uniquement aux contrats de vente à distance. Ceux-ci doivent donc porter sur des biens (ou des biens et des services, mais pas des services seuls), dont la propriété est transférée contre le paiement d'un prix. La conclusion du contrat doit intervenir sans la présence physique et simultanée des parties (par exemple à travers un site de commerce électronique).

Avec cette proposition de directive, la Commission ne se limite pas à imposer les mêmes règles sur tout le territoire de l'Union (puisqu'elle est d'harmonisation maximale): elle veille également à renforcer la protection du consommateur. Par rapport aux règles actuellement en vigueur en Belgique, on pointe notamment les différences suivantes:

– Actuellement, la garantie des biens de consommation est de deux ans. La loi présume néanmoins, sauf preuve contraire, que le défaut de conformité qui apparaît dans un délai de six mois à partir de la délivrance existait déjà à ce moment (art. 1649*quater*, § 3, C. civ.). Ce renversement de la charge de la preuve est particulièrement favorable au consommateur. Dans la proposition de directive, le délai de 6 mois est porté à 2 ans (art. 8, § 3, de la

proposition de directive). Ce sera donc au vendeur de démontrer, pendant ces deux ans, que le défaut n'existait pas au moment de la délivrance.
– De même, contrairement à ce que prévoit l'article 1649quater, § 2, Code civil, il ne sera plus permis d'imposer un délai dans lequel le consommateur est tenu d'informer le vendeur du défaut de conformité.

S'il faut saluer le renforcement de la protection des consommateurs, on regrette qu'une différence de traitement soit créée entre les ventes en ligne et les vente à distance de biens, d'une part, qui sont visées par cette proposition de directive, les autres ventes, qui demeurent soumises au régime traditionnel de la garantie des biens de consommation (directive 1999/44/CE et art. 1649*bis* et s. du C. civ.). Or, il n'est pas raisonnablement justifié de protéger davantage le consommateur qui s'engage en ligne. Il eût été préférable, d'après nous, de revoir tout le régime de la garantie des biens de consommation, sans faire de différence selon le mode de conclusion du contrat. Du reste, c'est en ce sens que la proposition a été revue et modifiée à l'automne 2017[24].

Question 1.2.4.
On comprend, à la lecture de la note de bas de page figurant en fin de question, que celle-ci a pour objet d'évaluer le caractère d'harmonisation maximale des directives adoptées dans le domaine de la protection des consommateurs.

Avec les directives d'harmonisation minimale adoptées précédemment en droit de la consommation, on a pu constater des différences importantes entre les législations des Etats membres. Dans le domaine du commerce en ligne, qui opère généralement par-delà les frontières des Etats membres, cela constitue un obstacle sérieux à la mise en place d'un marché unique numérique. Aussi faut-il promouvoir cette manière de faire, tout en étant conscient que, dans certains Etats membres, cela peut parfois conduire à une réduction du niveau de protection des consommateurs (qui étaient, le cas échéant, mieux protégés sous l'empire de la législation nationale précédente).

Il faut toutefois se rappeler que, nonobstant le caractère d'harmonisation maximale, certaines questions restent généralement de la compétence des Etats membres. On songe en particulier aux sanctions civiles ou pénales susceptibles d'être prononcées en cas de non-respect des règles adoptées. Or, la sanction ou, de manière générale, les procédures susceptibles d'être mises en œuvre en cas de méconnaissance des règles participent de l'effectivité de celles-ci. Sauf à

[24] Proposition modifiée de directive du Parlement européen et du Conseil concernant certains aspects des contrats de ventes de biens modifiant le règlement CE 2006/2004 du Parlement européen et du Conseil et la directive 2009/22/CE du Parlement européen et du Conseil et abrogeant la directive 1999/44/CE du Parlement européen et du Conseil, COM(2017) 637 final.

prévoir des mécanismes permettant de sanctionner un prestataire pour sa pratique sur tout le territoire de l'Union, il restera des différences et un risque de *forum shopping* des prestataires, tentés de s'établir dans un Etat réputé pour le faible niveau des sanctions ou des poursuites.

La multiplication des textes – et leur modification fréquente – tend également à rendre plus complexe le cadre normatif à respecter, ce qui complique la tâche des entreprises et, au final, n'assure pas nécessairement un niveau élevé de protection au bénéfice des consommateurs. Sans doute l'adoption d'un Code européen de droit de la consommation pourrait-elle contribuer à simplifier les règles, tout en contribuant à une meilleure articulation des textes.

Question 1.2.5.

On comprend que la question concerne les places de marchés électroniques, dont le but est notamment de mettre en relation des cocontractants potentiels, spécialement dans un environnement 2.0 marqué par l'essor de l'économie collaborative.

Pour autant qu'elles s'appliquent à la plateforme (ce qui est normalement le cas), ces directives offrent au consommateur un bon niveau de protection, en tout cas d'un point de vue théorique. On souligne en effet que l'existence de seules règles matérielles de protection est insuffisante si elle n'est pas accompagnée de sanctions effectives, proportionnées et dissuasives, et de règles de procédures permettant de les mettre en œuvre (en privilégiant, de préférence, les modes alternatifs de règlement de différends).

Nous n'avons pas connaissance de décisions de jurisprudence dans lesquelles des consommateurs se plaindraient de la méconnaissance de règles de protection de la part des plateformes en tant que telles. Les litiges se développent plus généralement à l'occasion de la relation contractuelle nouée, grâce à la plateforme, entre les consommateurs ou entre le consommateur et l'entreprise (parce que le bien commandé n'a pas été livré, ou qu'il est défectueux, etc.)[25]. Du reste, les plateformes veillent généralement à se prémunir contractuellement en insérant dans leurs conditions générales des clauses limitatives ou exonératoires de responsabilité, et en stipulant qu'en aucune manière elles ne sont parties au contrat C2C ou B2C conclu à travers la place de marché. Elles veillent ainsi à conserver un statut d'«intermédiaire» qui les autorise, par ailleurs, à bénéficier des exonérations de responsabilité établies par la directive sur le commerce électronique (transposée en Belgique dans le livre XII du Code de droit économique). A l'analyse, on constate d'ailleurs que ces activités d'intermédiation, qui ressortissent généralement au courtage, sont peu réglementées, sauf dans certains secteurs spécifiques (en matière de voyage, de finance, de crédit, etc.).

[25] Voy. par ex. Liège 25 mars 2011, *R.D.T.I.*, 2012/46, p. 67, note J.F. Henrotte ou Gand, 26 mai 2010, *D.C.C.R.*, 2011/91, p. 51, note C. Cauffman.

Cette manière de faire n'est probablement pas critiquable. Dans certaines situations, et en respectant le principe de proportionnalité, on pourrait toutefois souhaiter une intervention complémentaire du législateur pour imposer davantage d'obligations à la place de marché électronique, en particulier pour s'assurer que les personnes qu'elle met en relation respectent les obligations légales – de protection des consommateurs – qui leur incombent ou par des dispositifs techniques les empêchant de violer certaines exigences.

Question 1.2.6.

Les litiges initiés par les consommateurs devant les juridictions belges sont rares. En général, l'objet n'est pas de critiquer, en tant que telles, les conditions générales, même si, en fonction du cas d'espèce, cet élément peut faire l'objet d'un examen par le juge[26]. Plus souvent, c'est l'entreprise qui introduit une procédure judiciaire contre le consommateur, pour lui réclamer le paiement de prestations exécutées à la suite d'un contrat conclu en ligne (une entreprise de télécommunications ou un fournisseur, d'énergie, par exemple). Le Juge de paix saisi du litige pourra alors se pencher sur le respect, par l'entreprise, des règles de protection du consommateur, ce qui peut l'amener à examiner les conditions générales de l'entreprise, et/ou leur opposabilité au consommateur.

Ces conditions contractuelles peuvent également être examinées, à l'aune du droit de la consommation, dans le cadre d'actions en cessation commerciale entre entreprises où l'une reproche à l'autre de méconnaître les règles de protection des consommateurs (ce qui peut constituer un acte de concurrence déloyale).

Des mesures peuvent enfin être prises par les agents du SPF Economie dans le cadre des compétences qui leur reviennent conformément au livre XV du Code de droit économique (avertissement, proposition de transaction, transmission au parquet).

La manière dont les conditions générales sont rédigées par les prestataires (les GAFA en particulier), pour être ensuite mises à la disposition des consommateurs (moyennant un lien hypertexte), et acceptées par ceux-ci (par une case à cocher) constitue assurément un problème. On sait en effet que les consommateurs lisent rarement les conditions à ce stade (et, à supposer qu'ils le fassent, le mode de rédaction – long, complexe, très juridique – pourrait en tout état de cause les en dissuader). Aussi faut-il encourager les réflexions susceptibles de mener à une meilleure transmission (et acceptation) des informations essentielles à fournir au consommateur pour garantir un consentement éclairé de sa part, le cas échéant en s'inspirant de techniques promues dans le domaine de la protection des données à caractère personnel (*privacy by design* ou *privacy by*

[26] Voy. Civ. Liège, 1er octobre 2008, *DAOR*, 2009, p. 320, note E.

default, par exemple) ou en établissant un formulaire standard, court, simple et facilement compréhensible, sur lequel seules les données les plus importantes seraient reprises.

Question 1.2.7.
Les règles de protection des consommateurs sont principalement justifiées par la faiblesse présumée de ceux-ci lorsqu'ils s'engagent avec des professionnels. On considère en effet qu'ils souffrent d'un manque de connaissances sur des éléments de fait ou de droit du rapport contractuel, ou qu'ils peuvent être victimes d'abus de la part de leur cocontractant (clauses abusives, pratiques commerciales déloyales, etc.).

Les règles de protection des consommateurs ne devraient donc être étendues aux entreprises dans leurs relations avec d'autres entreprises que s'il est démontré que celles-ci souffrent également d'une telle position d'infériorité. Pour certaines entreprises, la faiblesse est normalement avérée: on pense par exemple au médecin qui contracte une assurance pour sa pratique professionnelle et qui n'est pas moins «faible» que quand il souscrit la même assurance à des fins privées. C'est par contre plus discutable s'il s'agit d'une banque, qui dispose d'un service juridique composé de plusieurs dizaines de personnes. Pour celles-ci, la théorie générale des contrats et des obligations, avec la souplesse qu'elle permet, est nettement plus adaptée.

Aussi faut-il limiter l'application éventuelle des règles de protection des consommateurs à un nombre limité et clairement circonscrit de professionnels, dont la faiblesse est difficilement contestable. Une telle possibilité est d'ailleurs expressément prévue dans la directive 2011/83/UE sur les droits des consommateurs, au considérant n° 13: «les États membres peuvent, par exemple, décider d'étendre l'application des règles de la présente directive à des personnes morales ou physiques qui ne sont pas des « consommateurs » au sens de la présente directive, comme les organisations non gouvernementales, les jeunes entreprises ou les petites et moyennes entreprises». La question pourrait d'ailleurs se poser de savoir s'il ne serait pas opportun d'imposer une telle extension du champ d'application de la directive.

1.3. Blocage géographique

Aux termes de l'article 18 du règlement 1215/2012, « l'action intentée par un consommateur contre l'autre partie au contrat peut être portée soit devant les juridictions de l'Etat membre sur le territoire duquel est domiciliée cette partie, soit, quel que soit le domicile de l'autre partie, devant la juridiction du lieu où le consommateur est domicilié ». Cette disposition s'applique à tout contrat conclu par un consommateur « lorsque (...) le contrat a été conclu avec une personne

qui exerce des activités commerciales ou professionnelles dans l'Etat membre sur le territoire duquel le consommateur a son domicile ou qui, par tout moyen, dirige ces activités vers cet Etat membre (...) ».

En application de ces dispositions, la simple accessibilité sur le territoire d'un Etat membre du site internet d'une entreprise ne peut, en soi, suffire à justifier la compétence des juridictions de cet Etat membre. Selon la Cour de justice, il importe en effet de rechercher si, au travers notamment de son site internet, il existe des indices de ce que l'entreprise envisageait de commercer avec des consommateurs situés sur le territoire de l'Etat membre où l'action est introduite.

Le règlement en projet poursuit l'objectif de prévenir la discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans les transactions commerciales transnationales entre professionnels et clients. Il interdit aux entreprises de bloquer ou de limiter l'accès des clients à leur interface en ligne pour des motifs liés à ces considérations.

Il est expressément stipulé à l'article 1er, §5, du nouveau règlement que le fait de se conformer à celui-ci ne saurait être interprété comme le signe qu'un professionnel dirige ses activités vers l'Etat membre où le consommateur a sa résidence habituelle au sens de l'article 17 du règlement 1215/2012. Rien n'est, par contre, stipulé quant à savoir si, en cas de vente passive, l'entreprise «exerce des activités commerciales ou professionnelles» dans l'Etat membre du consommateur. Il conviendrait de clarifier ce point.

A défaut, deux interprétations semblent possibles, l'une excluant qu'une vente passive donne compétence aux juridictions de l'Etat membre du consommateur, l'autre interdisant de déduire de l'obligation de permettre les ventes passives que l'entreprise dirige nécessairement ses activités vers l'Etat membre du consommateur, mais n'excluant pas, en cas de litige au sujet d'une vente passive, que la compétence des juridictions de l'Etat membre du consommateur soit reconnue au titre de l'exercice d'activités dans cet Etat membre.

Dès lors que l'objectif du règlement est d'intensifier le commerce électronique transnational au sein de l'Union européenne, cette incertitude pourrait générer une insécurité juridique dans les litiges présentant un élément d'extranéité. Ceci pourrait présenter un caractère inconfortable pour certaines entreprises, en les confrontant au risque d'une explosion des litiges en dehors de leur Etat-membre, et en augmentant, en conséquence, le coût du développement de leurs activités en ligne.

2. Médias numériques

Question 2.1.

En Belgique, le critère de «l'objet principal» dégagé dans l'arrêt susmentionné de la Cour de Justice était déjà appliqué par les régulateurs (Conseil Supérieur

de l'Audiovisuel, ci-après CSA, Vlaamse Regulator voor de Media, ci-après VRM, et Medienrat der Deutschsprachigen Gemeinschaft Belgiens, ci-après MRat) depuis plusieurs années[27]. La question de la compétence matérielle des régulateurs, en ce qui concerne les éléments audiovisuels présents sur les sites internet des médias remplissant le critère de «l'objet principal», était donc déjà tranchée. A cet égard, il est notamment possible de se référer à la recommandation relative au périmètre de la régulation des services de médias audiovisuels adoptée par le CSA en 2012, laquelle liste les critères sur base desquels cet organe établit sa compétence[28].

Cet arrêt a toutefois été accueilli par les régulateurs belges avec enthousiasme, car il a permis de consolider une pratique déjà existante, et a apporté confirmation des principes appliqués, bien que de façon plus nuancée[29]. Par ailleurs, cette confirmation jurisprudentielle concorde avec la position adoptée par les régulateurs belges au sein du groupe des régulateurs européens des services de médias audiovisuels (ci-après, ERGA).

Depuis lors, bon nombre de journaux en ligne belges (Le Soir, L'écho, ...) ont fait évoluer la présentation de leurs contenus, et incluent leurs contenus audiovisuels non plus sous forme de catalogues de vidéos, mais bien à la suite des articles détaillés correspondant à ces contenus; au contraire de médias tels que La Libre, ou encore la Dernière Heure. Les contenus audiovisuels présentés sur les sites internet des premiers ne sont, de la sorte, pas soumis aux obligations découlant de la directive SMAV, à l'opposé des seconds.

Cependant, certains de ces journaux en ligne renvoient aux contenus audiovisuels qu'ils fournissent en ligne par le biais d'hyperliens à destination de plateformes externes, par exemple Dailymotion. Dès lors, puisqu'il est possible d'accéder à ces plateformes sans passer par le site internet du média publiant le contenu audiovisuel dont question – et donc d'accéder à des catalogues de contenus audiovisuels comportant une ligne d'édition sur ces plateformes externes (du style chaine YouTube) –, la question de la compétence des régulateurs et l'application du critère de «l'objet principal» doivent de nouveau être examinées.

Question 2.2.

A l'heure actuelle, la Belgique ne dispose pas de règles sectorielles relatives aux plateformes audiovisuelles.

[27] Voy. notamment Conseil Supérieur de l'Audiovisuel, Bilan nouveaux médias, janvier 2013, disponible à l'adresse http://www.csa.be/documents/1962.

[28] Conseil Supérieur de l'Audiovisuel, Recommandation relative au périmètre de la régulation des services de médias audiovisuels, mars 2012, disponible à l'adresse http://csa.be/breves/652.

[29] Ibidem.

L'inclusion de ces plateformes dans le champ d'application des règles SMAV est en effet un pas dans la bonne direction, car cette reconnaissance légale permettra d'assurer un certain «level playing field»[30] entre les acteurs présents sur le marché. Ceci étant, les termes «plateformes de partage de vidéo» (video sharing platforms) pourraient assez rapidement poser problème, car d'autres types de plateformes pourraient remplir un rôle similaire[31] (par exemple, les réseaux sociaux, dont l'inclusion n'était pas envisagée dans la proposition originelle de révision de la directive). De la sorte, l'utilisation d'un terme plus englobant pourrait s'avérer plus pertinente, car moins facilement dépassé par l'évolution de la technologie.

A cette fin, le régulateur belge francophone (CSA) mentionne la notion de «distributeur de services de médias audiovisuels»[32], laquelle préexiste en Belgique, France, en Espagne, et aux Pays-Bas.

En ce qui concerne les obligations liées à la règlementation SMAV qui devraient s'appliquer auxdites plateformes de partage de vidéo, il est certain que leur rôle actif – mais limité – en matière éditoriale (par exemple, par le biais des recommandations aux utilisateurs, lors du visionnage de contenu généré par d'autres utilisateurs (ci-après UGC) doit impliquer à tout le moins de respecter les règles relatives à la protection des mineurs et la lutte contre les discours de haine. A l'heure actuelle, ces plateformes ont de toute façon un intérêt à se conformer à ces types de règles, ne serait-ce que pour leur image de marque.

En ce qui concerne d'éventuelles obligations complémentaires qui seraient imposées par la directive SMAV, une fois révisée, à ces acteurs, une application distributive devrait être prévue par le texte légal. De la sorte, en fonction de l'(intensité de l') activité éditoriale réellement exercée, différentes obligations pourraient s'ajouter à celles imposées initialement. Ainsi, au plus l'activité éditoriale d'une plateforme comme YouTube est importante vis-à-vis d'un (ensemble de) contenu(s), plus elle devrait se conformer à un nombre élevé d'obligations en matière de publicité, parrainage, ... jusqu'à parvenir à une situation juridique équivalente à celle d'un fournisseur de services de médias en cas de contenus propres à ladite plateforme (level playing field).

[30] Conseil Supérieur de l'Audiovisuel, *L'accès aux médias audiovisuels. Plateformes et enjeux.*, 2016, pp. 68 et 92, disponible à l'adresse http://colloque2016.csa.be/pages/259.

[31] *Ibidem*, pp. 14 et s.

[32] Définie à l'article 1er du décret de la Communauté française du 27 février 2003 sur la radiodiffusion, *M.B.*, 17 avril 2003. Ce texte ayant été revu à plusieurs reprises, il est renvoyé pour plus de facilité à la version coordonnée du 8 juin 2016 (officieuse) publiée par le CSA sur son site officiel: http://www.csa.be/system/documents_files/1440/original/D%C3%A9cret%20SMA%20coordonn%C3%A9%20au%208%20juillet%202016.doc.pdf?1474623093.

L'imposition d'obligations autres que celles portant sur la protection des mineurs et les discours de haine, par défaut et sans avoir égard à l'intensité du rôle éditorial joué par ces plateformes, aurait pour conséquence un risque accru d'atteinte à la liberté d'expression et d'information des internautes, d'autant plus maintenant que la proposition de directive discutée est considérée comme étant d'harmonisation minimale; et non plus d'harmonisation maximale, ce qui confèrera *de facto* une plus grande latitude aux différents régulateurs nationaux (dont l'indépendance vis-à-vis du pouvoir politique n'est pas toujours certaine) dans la mise en application du texte légal et des obligations en découlant.

Question 2.3.

Dans l'ordre juridique belge, deux cas sont particulièrement pertinents dans le cadre de cette question spécifique. Il s'agit d'une part, du cas RTL Group – S.A. TVi (chaines télévisées RTL-TVI et Club-RTL, ainsi que Plug-RTL plus récemment), et d'autre part du cas TF1.

En ce qui concerne le premier, l'entreprise RTL Group a installé son siège social au Luxembourg en 2008, tout en disposant de bureaux et d'effectifs à Bruxelles par le truchement d'une filiale, la S.A. TVi, et en diffusant notamment ses contenus à destination de la population belge francophone. Le CSA a dès lors tenté d'affirmer sa compétence matérielle en ce qui concernait les manquements à la législation belge à l'encontre des chaines RTL-TVI et Club-RTL, ainsi que les instructions subséquentes, en se fondant sur l'article 2 de la directive SMAV[33].

Suite à cela, des contestations de la part de RTL Group sont survenues, cette dernière précisant qu'elle relevait de la compétence exclusive de l'Autorité Luxembourgeoise Indépendante de l'Audiovisuel (ci-après, ALIA) et un arrêt a été rendu par le Conseil d'Etat belge le 15 janvier 2009[34] en la matière, lequel n'a cependant pas tranché le litige quant à l'interprétation de l'article 2 de la directive SMAV, ni accepté de poser de question préjudicielle à la Cour de Justice. Cet arrêt a néanmoins annulé les décisions administratives prises par le CSA à l'encontre de RTL Group.

En conséquence, un accord a été conclu en 2010 entre le Collège d'Autorisation et de Contrôle (CAC) du CSA et l'ALIA, afin de transmettre tous les cas relatifs à RTL Group qui poseraient problème en Belgique, à l'ALIA – de telle sorte qu'un régulateur puisse au moins se charger de ces derniers. La situation a néan-

[33] A titre indicatif, à l'heure actuelle 600 personnes travaillent à Bruxelles pour le compte de RTL Belgium s.a., anciennement s.a. TVi.

[34] C.E. (15e ch.), 15 janvier 2009, n°189.503, s.a. TVi et s.a. CLT-UFA – CSA, disponible à l'adresse http://www.raadvst-consetat.be/Arrets/189000/500/189503.pdf#xml=http://www.raadvst-consetat.be/apps/dtsearch/getpdf.asp?DocId=13497&Index=c%3a%5csoftware%5cdtsearch%5cindex%5carrets%5ffr%5c&HitCount=2&hits=13+14+&01542520181515.

moins à nouveau évolué en 2017, l'accord susmentionné ayant été rompu suite à une procédure interne au CSA, de telle sorte que ce dernier considère qu'il est le régulateur compétent vis-à-vis de RTL-TVI et Club-RTL, ainsi que de Plug-RTL[35]. RTL Group conteste toujours cette compétence[36].

En ce qui concerne le second cas, relatif à TF1, ce prestataire de services de médias audiovisuels établi en France n'a pas été considéré par le régulateur belge (CSA) comme étant susceptible de se voir appliquer l'article 2 de la directive SMAV, mais bien l'article 4. Cependant, les difficultés de mise en œuvre de la procédure y relative (seconde phase, § 3 de cet article), notamment la difficulté d'obtenir la preuve qu'un prestataire s'est établi dans un autre état membre pour échapper aux règles nationales en vigueur, l'ont rendu dans le cas présent inapplicable – puisque TF1 n'est pas installée à Paris pour contourner les règles belges, mais pratique néanmoins un ciblage du marché belge.

De façon plus générale, une critique générale émise par les régulateurs belges porte sur le principe du pays d'origine lui-même; et ce, au vu des différences de sensibilité en ce qui concerne la portée de la culture et des valeurs que chaque Etat membre (régulateur) souhaite protéger au premier plan.

Au titre de piste de réflexion, il est envisageable de penser des mécanismes de coopération entre régulateurs des Etats membres «cibles» des contenus audiovisuels transmis, ces régulateurs étant placés sur un pied d'égalité lors de la détermination des principes et méthodes régulatoires adoptés ensuite de commun accord, et appliqués par catégories de contenus (documentaires, divertissements, actualités, ...).

Enfin, les régulateurs belges ne recensent pas d'affaire(s) pertinente(s) relative(s) à des prestataires établis en dehors de l'Union européenne, car ces derniers s'adressent à un public relativement restreint, et ce sans ciblage significatif du marché belge.

Question 2.4.

A titre de considération liminaire, il peut être utile de préciser ici que la directive SMAV mentionne, en ses versions en langue française et anglaise, le qualificatif «indépendants» à deux reprises en matière d'organismes de régulation nationaux.[37] Bien que ce qualificatif n'y ait qu'une incidence juridique limitée,

[35] A cet égard, voy. notamment le communiqué de presse du CSA relatif à l'instruction lancée en 2017 à l'encontre de CLT-UFA, disponible à l'adresse http://www.csa.be/breves/1171; ainsi que les articles de presse y relatifs, notamment Le Soir, Instruction du CSA contre RTL, 10 octobre 2017, disponible à l'adresse https://www.rtbf.be/info/medias/detail_le-csa-ouvre-une-instruction-contre-rtl-et-l-emission-maries-au-premier-regard?id=9732362.

[36] Ibidem.

[37] Il s'agit du considérant 94 de ladite directive, ainsi que de son article 30.

il est intéressant de noter cette ambition d'indépendance pour les régulateurs nationaux, en germe dans le texte de la directive.

En ce qui concerne l'introduction d'exigences d'indépendance détaillées pour les régulateurs nationaux des médias au sein de la directive SMAV, il s'agirait bien sûr d'un pas en avant, voire même d'une nécessité. A cet égard, l'on peut envisager un régime inspiré de celui applicable aux Autorités Règlementaires Nationales (ci-après, ARN) en vertu de la règlementation relative aux communications électroniques.

A l'heure actuelle, en Belgique, les régulateurs des médias bénéficient déjà d'une certaine indépendance, que l'on peut qualifier de «partielle».

Les différents décrets SMAV belges, issus de chacune des Communautés, reconnaissent en effet légalement cette indépendance en faisant mention «d'autorités administratives indépendantes»[38]. Cependant, la nomination des membres des organes décisionnels de ces régulateurs (CSA, VRM et MRat) est majoritairement effectuée par les différents gouvernements des Communautés[39], et ce en fonction des affiliations politiques des candidats. De plus, les qualifications et expériences requises de la part des candidats aux postes ouverts dans ces organes décisionnels (par exemple, le CAC en ce qui concerne le CSA) ne sont pas ou peu précisées par les textes légaux, bien que cela ne semble pas avoir d'impact sur les profils sélectionnés *in fine*[40]. Par ailleurs, les méthodes de financement des régulateurs ne leur permettent pas une indépendance totale vis-à-vis des pouvoirs exécutifs et législatifs des Communautés dont ils ressortent[41].

[38] Décret de la Communauté française du 27 février 2003 sur la radiodiffusion tel que coordonné par le CSA, *op. cit.*, article 133; Décret de l'Autorité flamande du 27 mars 2009 concernant la radiodiffusion et la télévision, *M.B.*, 30 avril 2009, articles 215 et 218. Ce texte ayant été revu à plusieurs reprises, il est renvoyé pour plus de facilité à la version coordonnée du 3 février 2017 (officieuse) publiée par le VRM sur son site officiel : https://www.vlaamseregulatormedia.be/sites/default/files/geconsolideerde_tekst_van_het_mediadecreet_van_27_maart_2009_-_bijgewerkt_tot_3_februari_2017.pdf; et Décret de la Communauté germanophone du 27 juin 2005 sur la radiodiffusion et les représentations cinématographiques, *M.B.*, 6 septembre 2005, article 86. Ce texte ayant été revu à plusieurs reprises, il est renvoyé pour plus de facilité à la version coordonnée du 28 mars 2017 (officieuse) publiée par le MRat sur son site officiel : http://medienrat.be/files/Dekret_27_Juni_2005_Stand_28_Maerz_2017.pdf.

[39] ICRI, KU Leuven; Cullen International; *et al.*, Etude INDIREG (Indicators for independence and efficient functioning of audio-visual media services regulatory bodies), Annex II – Country Tables – Belgium, commanditée par la Commission européenne, 2011, pp. 17-18, disponible à l'adresse http://www.indireg.eu/files/Annex_II-_CountryTables_Belgium.pdf.

[40] Institut de droit européen des médias et Université du Luxembourg, Etude RADAR (AudioVisual Media Services- Regulatory Authorities' InDependence And Efficiency Review), commanditée par la Commission européenne, 2015, p. 47, disponible à l'adresse https://ec.europa.eu/digital-single-market/news/study-audiovisual-media-services.

[41] ICRI, KU Leuven; Cullen International ; *et al.*, Etude INDIREG, Annex II – Country Tables – Belgium, *op. cit.*, pp. 31-32.

En ce qui concerne les antécédents relatifs à des pressions politiques ou commerciales indues, il faut remarquer que la procédure même de nomination des membres des organes décisionnels des régulateurs implique des possibles pressions politiques sur lesdits régulateurs, ultérieurement. Qui plus est, les différents gouvernements de Communautés disposent du pouvoir de donner des instructions aux régulateurs nationaux relevant de leur compétence[42]. De la sorte, il semblerait qu'à plusieurs occasions, des pressions politiques aient été subies – à tout le moins par le CSA – à des fins d'avancement politique des donneurs d'ordres.

Ceci étant, il n'existe en Belgique aucun obstacle juridique de nature à poser problème à l'instauration d'une indépendance concrète des régulateurs nationaux. Il existe de plus, dans le chef de ces régulateurs, la volonté d'une indépendance réelle, au niveau des nominations, ainsi qu'aux niveaux financier, politique, structurel, ...

Il est probable qu'un régime juridique permettant de parvenir à une telle indépendance tant sur le plan légal, que sur le plan factuel, permettrait de favoriser la création d'un marché unique pour les services de médias audiovisuels. En effet, cela pourrait mener à une application plus libre et consciencieuse des textes légaux européens et de leurs transpositions nationales par les régulateurs, notamment en leurs composantes relatives au marché unique.

Question 2.5.

Parmi les questions qui ont causé le plus de controverses en Belgique, en ce qui concerne l'application des lois de radiodiffusion, les régulateurs belges s'accordent à citer les règles sur les communications commerciales – notamment en ligne –, et les règles de protection des mineurs; ces deux thématiques étant, toutefois, maintenant balisées dans une certaine mesure[43],[44].

La seconde de ces problématiques se décline au travers plusieurs volets: les questions relatives à l'identification des mineurs lors de la fourniture de contenus audiovisuels en ligne (ou sous forme de services télévisuels non-linéaires) qui sont destinés à un public majeur ou, à tout le moins, averti; et les questions d'opportunité en matière de signalétique destinée à prévenir en dessous de quel âge le contenu diffusé est déconseillé.

Pour les questions d'identification préalable des mineurs, dans le cas de fourniture de contenus en ligne (ou sous forme de service télévisuel non-linéaire) non adaptés à ces derniers, la pratique actuelle est focalisée sur des moyens

[42] Institut de droit européen des médias et Université du Luxembourg, Etude RADAR, *op. cit.*, p. 72.

[43] Voy. notamment Conseil Supérieur de l'Audiovisuel, Recommandation relative aux communications commerciales sur les plateformes Internet, novembre 2015, disponible à l'adresse http://www.csa.be/documents/2530.

[44] Voy. notamment Conseil Supérieur de l'Audiovisuel, Recommandation relative à la protection des mineurs, février 2014, disponible à l'adresse http://www.csa.be/documents/2230.

techniques tels que l'introduction d'un numéro de carte de crédit, ou encore d'un code parental pour débloquer la possibilité de visionner tout contenu soumis à des restrictions en fonction de l'âge[45].

En matière de signalétique, des désaccords sont encore survenus récemment entre le régulateur francophone et la RTBF. En l'espèce, la diffusion litigieuse concernait l'émission «Retour aux sources», laquelle montrait des images d'archive de la chute du (troisième) Reich; ces dernières contenant des photos de charniers, ou encore des plans prolongés de victimes de viols. Cette émission passant à 20h00 et sans signalétique, des plaintes ont été enregistrées par le CSA; ce à quoi la RTBF objectait qu'une telle émission était tellement intéressante et enrichissante, qu'il n'aurait pas été judicieux de potentiellement exclure une partie de l'audience lors de la diffusion par le biais d'une signalétique déconseillant le visionnage en dessous d'un certain âge.

Les deux volets de cette thématique sont toutefois aujourd'hui de moins en moins souvent problématiques, comme en témoigne l'avis «Protection des mineurs» émis en 2017 par le CSA[46].

En ce qui concerne l'opportunité de procéder à l'harmonisation de certains domaines par le biais de la révision de la directive SMAV, certaines matières devraient assurément être envisagées, notamment les règles relatives à la concentration des médias, ou encore relatives aux placements de produits. D'autres, par contre, qui touchent plus spécifiquement les sensibilités nationales des populations des différents états membres – lesquelles divergent quant à certains contenus – devraient être laissées à la libre appréciation des autorités régulatoires nationales indépendantes. Ainsi, le contenu diffusé par la RTBF dans l'exemple mentionné ci-dessus ne rencontrerait pas le même écho auprès de toutes les populations de l'UE, et mériterait de ce fait une approche différenciée en matière de protection des mineurs dans les différents états «ciblés».

Question 2.6.

Des initiatives en matière de publicité ciblée à la télévision existent déjà en Belgique, et sont principalement le fait des entreprises Telenet et Proximus. Ces dernières ont ainsi procédé à l'émission de publicité ciblée «sur la base des habitudes télévisuelles et/ou de navigation personnelle du client»[47].

[45] Arrêté du Gouvernement de la Communauté française du 21 février 2013, relatif à la protection des mineurs contre les programmes télévisuels susceptibles de nuire à leur épanouissement physique, mental ou moral, *M.B.*, 11 mars 2013, article 2, §§ 1 et 3.

[46] Conseil Supérieur de l'Audiovisuel, Avis protection des mineurs – 2016, juillet 2017, disponible à l'adresse http://www.csa.be/documents/2749.

[47] Commission de la Protection de la Vie Privée, Communiqué de presse: *Résultat de l'examen porté sur la publicité télévisée personnalisée de Telenet et Proximus*, 19 juillet 2017, disponible à l'adresse https://www.

Ces agissements n'ont pas été considérés par les régulateurs de SMAV nationaux; mais bien par la Commission de la Protection de la Vie privée (ci-après, CPVP), qui est l'autorité belge de protection des données à caractère personnel et de la vie privée instituée par la loi du 8 décembre 1992, relative à la protection de la vie privée[48].

Cet organe avait au préalable balisé les conditions dans lesquelles un traitement de données à caractère personnel permettant de diffuser de la publicité ciblée à la télévision pouvait s'effectuer en conformité avec la législation vie privée belge, par le biais de deux avis[49]. Cependant, certaines questions se sont posées lorsque l'entreprise Telenet a initié de telles pratiques, notamment en ce qui concerne les modalités d'obtention du consentement des personnes concernées à voir leurs données traitées pour une finalité de marketing direct (à savoir, le choix d'un mécanisme «opt-in» ou «opt-out»)[50].

Bien qu'à l'heure actuelle, la CPVP ne dispose pas (encore[51]) d'un pouvoir de contrainte, ni de sanction, un dialogue s'est tenu entre les parties intéressées et a abouti à un accord que ladite Commission juge équilibré; à savoir: «la Commission vie privée ne s'oppose pas par principe à de nouvelles formes de publicité ou de marketing direct mais tend toujours à un équilibre adéquat entre les intérêts économiques légitimes des entreprises et les intérêts du citoyen en termes de vie privée»[52]. Les «intérêts du citoyen» se rapportent ici notamment à la formalisation du consentement à obtenir par les responsables de traitements de données à caractère personnel pour effectuer du marketing direct, en particulier lorsque le RGPD sera applicable.

privacycommission.be/fr/news/resultat-de-lexamen-sur-la-publicite-televisee-personnalisee-de-telenet-et-proximus.

[48] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.

[49] Commission de la Protection de la Vie Privée, Avis n° 06/2006: *avis relatif à la télévision numérique et à la protection de la vie privée*, 7 février 2007, disponible à l'adresse https://www.privacycommission.be/sites/privacycommission/files/documents/avis_06_2007_0.pdf, et Commission de la Protection de la Vie Privée, Avis n° 29/2007 : *avis relatif aux nouveaux modes de consommation médiatique et à la protection de la vie privée*, 19 septembre 2007, disponible à l'adresse https://www.privacycommission.be/sites/privacycommission/files/documents/avis_29_2007_0.pdf.

[50] Commission de la Protection de la Vie Privée, Communiqué de presse : *La Commission vie privée examine les pratiques de marketing direct de Telenet : l' "opt-in" doit être la base*, 13 septembre 2016, disponible à l'adresse https://www.privacycommission.be/fr/news/la-commission-vie-privee-examine-les-pratiques-de-marketing-direct-de-telenet.

[51] Ce qui sera le cas lorsque la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.* 10 janvier 2018, sera applicable (25 mai 2018).

[52] Commission pour la Protection de la Vie Privée (CPVP), Communiqué de presse: *Résultat de l'examen porté sur la publicité télévisée personnalisée de Telenet et Proximus*, *op. cit.*

Il est intéressant de constater que le régulateur belge francophone des SMAV (CSA) se dit volontaire pour se coordonner avec la CPVP en la matière, dès lors que la réforme de cette dernière – liée à l'applicabilité du RGPD – sera effective.

Une approche européenne harmonisée pourrait être pertinente en la matière, mais uniquement si des mécanismes de coopération nationale entre autorités de protection des données à caractère personnel et régulateurs de SMAV se révèlent insuffisants. Une autre voie pourrait être l'instauration d'un groupe de discussion européen entre ces deux types d'autorités, regroupant l'ERGA et les autorités de protection de la vie privée pour ces résoudre ces questions particulières.

Question 2.7.

En Belgique, le régime de la retransmission par câble tel que prévu par la directive 93/83/CEE est le plus appliqué, notamment pour les chaines dédiées au service public (RTBF, VRT, ...). Le régime prévu en ce qui concerne la radiodiffusion par satellite n'est quant à lui pas réellement appliqué, en ce sens que les prestataires établis en Belgique n'émettent pas particulièrement par le biais de liaisons satellites montantes.

Par ailleurs, en matière de réception des radiodiffusions opérées par satellite, la plupart des prestataires commerciaux (RTL, VTM, ...) procèdent conformément à la méthode dite de «l'injection directe», de telle sorte qu'un payement aux sociétés de gestion collective des droits d'auteurs n'est pas requis[53].

Le régime de retransmission par câble mentionné ci-dessus est effectivement encore pertinent, et l'obligation de conclure un contrat de licence avec une société de gestion collective de droits d'auteurs – que le moyen technique utilisé soit le câble, ou un satellite – a d'ailleurs été étendue, dans la législation belge transposant la directive 93/83/CEE, aux situations purement internes, n'impliquant pas d'élément d'extranéité[54].

Ce même régime a également été étendu en Belgique à l'IPTV, tant en ce qui concerne les situations transfrontières européennes que les situations nationales; mais pas aux transmissions en ligne des organismes de radiodiffusion, ce qui pose question d'un point de vue juridique.

Dans les faits, toutefois, les transmissions en ligne effectuées par ces prestataires semblent être soumises aux mêmes modalités, de par la pratique de la Société belge des auteurs, compositeurs et éditeurs (ci-après, SABAM)[55].

[53] C.J.U.E., arrêt SBS Belgium NV c. Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM), 19 novembre 2015, C-325/14, EU:C:2015:764.

[54] Code de Droit Economique (ci-après CDE), livre XI, articles XI.220 et s.

[55] A cet égard, voy. notamment l'accord conclu entre la SABAM et Google en 2012: SABAM, Communiqué de presse: *La SABAM et Google signent un contrat de licence numérique novateur*, 19 décembre

Quoi qu'il en soit, la proposition de règlement établissant des règles sur l'exercice du droit d'auteur et des droits voisins applicables à certaines diffusions en ligne d'organismes de radiodiffusion et retransmissions d'émissions de télévision et de radio[56] apparait comme étant à même d'apporter plus d'égalité de traitement et de sécurité juridique en la matière.

Question 2.8.

A titre de remarque préliminaire, il faut ici remarquer qu'il est encore très (trop) tôt pour déceler les obstacles nationaux potentiels à l'application de ce nouveau règlement. Néanmoins, il ne semble pas y avoir, à l'heure actuelle, de pierre d'achoppement ou d'obstacle particulièrement saillant en la matière.

En ce qui concerne le contrôle du pays de résidence du consommateur d'un service tel que ceux envisagés par le règlement dont question, il est certain que des vérifications doivent être opéréespar les prestataires ; et en ce qui concerne la fréquence de ces dernières, un nombre maximum de vérifications par année devrait être consacré par le texte légal, ou encore par un acte d'exécution. En la matière, une méthode efficace pourrait être l'instauration de contrôles à fréquence aléatoire (par exemple, des contrôles dont la fréquence serait déterminée aléatoirement par le biais d'un programme informatique dédié), jusqu'à atteindre le nombre de contrôles annuels fixé, qui pourrait tourner aux alentours de 2 ou 3. Le nombre de ces contrôles annuels devrait, quoi qu'il en soit, être déterminé en prenant en considération tous les facteurs pertinents, en ce compris le principe de minimisation des données imposé par le règlement général sur la protection des données (ci-après, RGPD).

Afin de se conformer au principe de minimisation des données mentionnée ci-dessus, et de le concilier avec le principe de contrôle – relativement fréquent – du pays de résidence des consommateurs concernés, la solution la plus simple semble être de procéder à ces vérifications sur base des données publiques en premier lieu, lorsque de telles données existent; la charge de l'actualisation de ces données reposant alors sur les différentes administrations compétentes en la matière.

Par ailleurs, l'obligation légale imposée aux prestataires de se limiter à deux des méthodes d'identification prévues par le règlement (lesquelles auront assurément été pensées dans l'optique du RGPD) permet déjà, dans une certaine mesure, de minimiser les données traitées par ces prestataires.

2012, disponible à l'adresse http://www.sabam.be/fr/press/la-sabam-et-google-signent-un-contrat-de-licence-numerique-novateur.

[56] Proposition de Règlement du Parlement européen et du Conseil du 14 novembre 2016, établissant des règles sur l'exercice du droit d'auteur et des droits voisins applicables à certaines diffusions en ligne d'organismes de radiodiffusion et retransmissions d'émissions de télévision et de radio, COM(2016) 594 final.

Enfin, la suppression des données à caractère personnel directement après la procédure de contrôle – en ne gardant dès lors que le résultat, positif ou négatif, du contrôle – permettrait également de parvenir dans une certaine mesure à minimiser les quantités et qualités de données à caractère personnel traitées, s'agissant de la conservation de ces dernières.

3. Infrastructures numériques

Question 3.1.

Avant l'adoption, au niveau européen, du règlement internet ouvert (ci-après RIO), applicable depuis fin novembre 2015, la Belgique s'était déjà dotée de certaines règles contribuant, de manière indirecte, à la neutralité de l'internet, comme l'article 113 § 4, de la loi belge relative aux communications électroniques (ci-après, LCE)[57], qui donne[58] le pouvoir à l'IBPT d'imposer des exigences minimales en matière de qualité des services aux fournisseurs de réseaux publics de communications électroniques afin prévenir la dégradation du service et l'obstruction ou le ralentissement du trafic sur leurs réseaux.

Plusieurs propositions législatives avaient également vu le jour afin d'implanter ce concept de façon contraignante dans l'ordre juridique belge, tant au sein de la LCE[59] que de la Constitution[60]. Néanmoins, ces propositions n'avaient pas abouti, faute de consensus politique à cet égard[61].

La grande nouveauté du RIO est qu'il interdit non seulement les discriminations classiques – dégradation de la qualité de services informatiques qui concurrencent les services du fournisseur d'accès à l'internet, mais également les discriminations *positives*, dont le cas emblématique est la «fixation de taux zéro», la non facturation du volume de données consommées par certaines applications informatiques spécifiques. L'IBPT, qui est chargé de la surveillance du respect des obligations du RIO en Belgique, examine, pour chaque offre spécifique,

[57] Loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005.

[58] Inséré par l'article 76 § 17 de la loi du 10 juillet 2012, amendement entré en vigueur le 4 aout 2012.

[59] Proposition de révision de la Constitution complétant l'article 23, afin de consacrer le principe de la neutralité du réseau Internet, *Doc. Parl.*, Chambre, 2010-2011, no 53-1471/1.

[60] Proposition de loi du 1er juin 2011 modifiant la loi du 13 juin 2005 relative aux communications électroniques, en ce qui concerne la neutralité du réseau, *Doc. parl.*, Chambre, 2010-2011, no 53-1536/001.

[61] En la matière, voy. O. BRAET, H. JACQUEMIN, R. QUECK, M. PIRON, L. SCHUMACHER, D. STEVENS et P. VALCKE, «La réglementation de la neutralité du réseau en Belgique – Réflexions et recommandations», *Revue du Droit des Technologies de l'Information*, 2014, n°54, pp. 5 et s., disponible à l'adresse https://lirias.kuleuven.be/bitstream/123456789/462838/1/La+r%C3%A9glementation+de+la+neutralit%C3%A9+en+Belgique_r%C3%A9flexions+et+recommendations.pdf, et M. PIRON, «La neutralité des réseaux et la garantie de la fourniture de services de médias audiovisuels», *Revue du Droit des Technologies de l'Information*, 2011, n° 45, pp. 69 et s., disponible à l'adresse http://www.rdti.be/Doc-Jur/doc45-3.html.

l'effet négatif potentiel sur le choix des utilisateurs finals[62]. Aucune offre avec taux zéro en Belgique n'avait cependant un tel effet négatif. «Globalement, l'IBPT pense qu'il n'y a pas de sérieux motifs de préoccupation en Belgique sur le plan de l'accès à un internet ouvert (d'autant plus que les volumes Internet inclus dans les offres des ISP sont sans cesse croissants, pour répondre à l'évolution du trafic de données croissant)»[63]. Le seul opérateur auquel l'IBPT a demandé de changer son offre est Lycamobile, qui rendait impossible le partage de connexion internet (thetering)[64].

Question 3.2.

En guise de remarque préliminaire, il faut ici préciser que la tendance actuelle est à la fragmentation du marché intérieur. Ainsi, le Conseil de l'IBPT a décidé le 30 mai 2016 d'imposer une amende administrative à Skype pour ne pas avoir notifié son service 'Skype Out' en tant que service de communication électronique[65]. L'obligation de notification énoncée à l'article 9 de la LCE[66] n'implique pas simplement l'obligation de remplir un formulaire de notification et le paiement d'une redevance unique et annuelle à l'IBPT, mais entraîne en outre la nécessité de se conformer à de nombreuses obligations.

En suivant cette logique, et puisque les applications informatiques qui permettent d'appeler des numéros de téléphone sont disponibles depuis toutes les connexions à internet dans le monde, Skype et les prestataires de services similaires seraient alors dans l'obligation de notifier leurs services dans chacun des Etats membres et d'adapter ceux-ci aux exigences applicables dans chacun de ces Etats.

Jusqu'alors, les applications informatiques étaient considérées comme des services de la société de l'information, et la directive sur le commerce électronique du 8 juin 2000[67] avait instauré un marché unique pour ces services en prévoyant

[62] IBPT, Rapport «L'analyse de l'IBPT du « zero-rating » d'applications dans les offres de Proximus», 30 janvier 2017, disponible à l'adresse http://www.bipt.be/fr/operateurs/telecom/protection-des-consommateurs/lanalyse-de-libpt-du-zero-rating-dapplications-dans-les-offres-de-proximus.

[63] IBPT, « Rapportannuel concernant la surveillance exercée sur la neutralité de l'internet en Belgique (période du 30 avril 2016 – 30 avril 2017)», 2017, p. 83 disponible à l'adresse http://www.bipt.be/fr/operateurs/telecom/protection-des-consommateurs/rapport-annuel-concernant-la-surveillance-exercee-sur-la-neutralite-de-linternet-en-belgique.

[64] IBPT, « Rapportannuel concernant la surveillance exercée sur la neutralité de l'internet en Belgique (période du 30 avril 2016 – 30 avril 2017)», *op. cit.*, p. 18.

[65] IBPT, Communiqué de presse: *L'IBPT impose une amende à Skype pour le service télécoms Skype Out*, 15 juillet 2016, disponible à l'adresse http://www.bipt.be/fr/operateurs/press-release/123-l-ibpt-impose-une-amende-a-skype-pour-le-service-telecoms-skypeout.

[66] Loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005.

[67] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans

que les prestataires de tels services tombaient uniquement sous le régime juridique du pays d'établissement. Une entreprise établie dans un pays de l'union pouvait ainsi fournir ses services dans l'ensemble de l'Union sans formalité additionnelle dans d'autres Etats membres.

L'interprétation extensive du concept de communications électroniques restreint dès lors cette liberté. A cet égard, il est d'autant plus inquiétant que la Commission a proposé un amendement de la définition des services de communications électroniques dans ce sens[68], visant à y inclure des applications informatiques telles que Skype ou Viber out.

Ceci étant, l'Union européenne devrait effectivement aller plus loin dans la création d'un marché unique pour les réseaux et services de communications électroniques; bien que différents freins existent – en sus de celui mentionné ci-dessus – vis-à-vis de cette ambition, dans l'hypothèse où elle serait mise en œuvre par le biais d'un régime d'octroi de licences à l'échelle européenne.

En effet, une telle question touche directement à la souveraineté nationale des Etats membres, dès lors qu'il est question de la création, sur leur territoire, d'infrastructures physiques ou encore de gestion du spectre. Il serait donc probablement plus facile d'envisager la chose en mettant en place un système de coopération entre les différents Etats membres (par exemple, grâce à une coopération renforcée).

De plus, un système d'octroi de licences à l'échelle européenne devrait être pensé de façon à inclure des obligations relatives aux objectifs minimaux à atteindre par les détenteurs desdites licences dans chaque Etat membre, afin d'éviter que seules les portions rentables du marché intérieur ainsi renforcé ne soient exploitées, au détriment des zones qui le sont moins. De la sorte, l'application des principes dits «de service universel» pourrait également bénéficier de ce renforcement du marché intérieur.

Par ailleurs, les sommes astronomiques requises pour faire aboutir de tels projets créent le risque que des licences attribuées à l'échelle de l'Union européenne ne puissent être conférées qu'à des entreprises ayant suffisamment de capital que pour ce faire ; ce qui ne favoriserait que les opérateurs déjà fortement implantés, au détriment d'entreprises moins puissantes ou de nouveaux entrants. Dans l'optique de favoriser la concurrence, le développement d'une voie alternative serait dès lors souhaitable, afin de permettre à des entreprises de plus petite taille de coopérer entre elles pour agir à l'échelle européenne, sans favoriser outre mesure les fournisseurs d'infrastructures et de services déjà solidement implantés et bénéficiant de ressources colossales

le marché intérieur (« directive sur le commerce électronique »), *J.O.C.E.*, n° L 178 du 17 juillet 2000.

[68] Proposition de directive établissant le code des communications électroniques européen (Refonte), COM/2016/0590 final – 2016/0288 (COD), article 2, point 6).

En ce qui concerne l'adoption de mesures spéciales de bande large par les autorités nationales, deux éléments sont à pointer ici:

- la transposition en droit belge de la directive 2014/61 est en cours[69]; et
- dans le contexte du réexamen de la régulation des marchés 3A et 3B, l'IBPT a laissé entrevoir dans une consultation que la régulation pourrait prendre en compte (être réduite en réaction à) des investissements dans le large bande (30 Mbps) et dans les zones blanches[70].

Question 3.3.

Les seuls litiges en matière d'assignation de spectre radio au cours des dernières années avaient trait à la bande de fréquences 3,5 GHz, et en particulier concernant l'utilisation par l'IBPT de la discrétion que la loi lui laisse, d'étendre ou non des autorisations existantes[71].

En parallèle, la multiplication des taxes imposées aux opérateurs de communications mobiles par les autorités locales et provinciales a continué de causer problème. Outre les impôts applicables à tous les agents économiques, tels l'impôt sur les sociétés ou la taxe sur la valeur ajoutée, les opérateurs de télécommunications supportent un ensemble de charges financières et fiscales spécifiques à ce secteur en Belgique.

La Cour de Justice a bien précisé que «(l)e cadre juridique garantissant la liberté de fournir des réseaux et des services de communications électroniques, établi par la directive « autorisation », serait privé d'effet utile si les États membres étaient libres de déterminer les charges fiscales que doivent supporter les entreprises du secteur»[72], mais la Cour a néanmoins admis que le droit de l'Union

[69] Centre de Presse international (service du Service public fédéral (SPF) Chancellerie du Premier ministre), Communiqué de presse: *Transposition de la directive relative à la réduction du coût des réseaux de communications électroniques: Conseil des ministres du 16 décembre 2016*, 16 décembre 2016, disponible à l'adresse http://www.presscenter.org/fr/pressrelease/20161216/transposition-de-la-directive-relative-a-la-reduction-du-cout-des-reseaux-de-c.

[70] IBPT, *Consultation concernant l'analyse des marchés du haut débit et de la radiodiffusion télévisuelle*, 7 juillet 2017, disponible à l'adresse http://www.ibpt.be/fr/operateurs/telecom/marches/large-bande/projet-de-decision-analyse-de-marche-2017/projet-de-decision-analyse-de-marche.

[71] Voy. notamment le recours du 23 mai 2017 de la société Citymesh contre la décision de l'IBPT de ne plus étendre la zone géographique de couverture d'autorisation accordée dans cette bande de fréquence. Cette bande de fréquence est en effet destinée aux communications mobiles selon la future norme 5G. Document disponible à l'adresse http://www.ibpt.be/public/files/nl/22277/Requ%C3%AAte%20en%20suspension%20et%20annulation%20de%20Citymesh%20aupr%C3%A8s%20de%20%20la%20Cour%20des%20March%C3%A9s%20contre%20la%20D%C3%A9cision%20du%20Conseil%20de%20l%E2%80%99IBPT%20du%2021%20mars%202017.pdf.

[72] C.J.U.E., arrêt *Vodafone Omnitel e.a.*, aff. jointes C-228/12 à C-232/12 et C-254/12 à C-258/12, EU:C:2013:495, point 36, ainsi que, par analogie, les arrêts *Albacom et Infostrada*, aff. jointes C-292/01 et C-293/01, EU:C:2003:480, point38, ainsi que *Telefónica de España*, C-284/10, EU:C:2011:513, point19.

ne s'opposait notamment pas à des redevances sur les antennes GSM si le «fait générateur»[73] n'est pas lié à la procédure d'autorisation[74].

Ce concept de fait générateur laisse une marge discrétionnaire aux pouvoirs locaux[75] pour contourner, en formulant d'une manière habile la base imposable, l'interdiction d'imposer des redevances additionnelles aux opérateurs de communications mobiles pour l'utilisation de fréquences pour lesquelles ils ont déjà payé une redevance à l'Etat fédéral. En effet, le but du placement d'antennes est évidemment d'utiliser les fréquences obtenues. Or les communes et provinces bénéficient déjà des revenus de la taxation des installations de mâts GSM au titre de l'impôt sur le revenu cadastral[76].

En outre, la question se pose du respect du principe de non-discrimination quand des antennes utilisées à d'autres fins ou des éoliennes ne sont pas grevées des mêmes redevances.

Une autre incertitude juridique qui demeure en Belgique pour les opérateurs de communications mobiles sont les normes réglementaires fixées en matière radiations non ionisantes[77]. La recommandation 1999/519/CE du Conseil du 12 juillet 1999[78] recommande une densité de puissance maximale, mais ce plafond n'est pas obligatoire. Les législateurs régionaux ont abaissé substantiellement ce seuil, certains plus que d'autre pour des raisons probablement non dénuées de considérations électoralistes.

L'absence de prévisibilité future du plafond génère une incertitude préjudiciable à la modernisation des réseaux et au déploiement de la technologie selon la nouvelle norme 5G, qui demandera un nombre encore plus important d'antennes.

[73] Par exemple «en raison de la présence sur le domaine public ou privé de mâts, de pylônes ou d'antennes de radiotéléphonie mobile nécessaires à leur activité, à une taxe générale sur les implantations», C.J.U.E., arrêt du 4 septembre 2014, *Belgacom* (C-256/13) et *Mobistar* (C-264/13) *c. Provincie van Antwerpen*. Voy. également C.J.U.E., arrêt du 17 décembre 2015, *Proximus SA, anciennement Belgacom SA c. Province de Namur*, C-517/13.

[74] C.J.U.E., arrêts du 27 juin 2013, *Commission/France*, C-485/11, EU:C:2013:427, points 30, 31 et 34, et *Vodafone Malta et Mobisle Communications*, C-71/12, EU:C:2013:431, points 24 et 25.

[75] L'article 98, § 2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques interdit aux communes de taxer, pour des motifs budgétaires ou autres, l'activité économique des opérateurs de télécommunications, mais la Cour constitutionnelle a jugé qu'une telle interdiction viole le principe de l'autonomie communale: C.C., arrêt du 15 décembre 2011, n° 189/2011.

[76] En effet, les revenus provenant de concessions pour l'installation de mâts GSM sont des revenus de biens immobiliers, matière imposable du précompte immobilier, qui avait été attribué aux régions par la loi spéciale de financement: C.C., arrêt du 19 juin 2014, n° 93/2014.

[77] Voy. C.C., arrêts du 27 janvier 2016, n° 12/2016 et n° 189/2011.

[78] Recommandation 1999/519/CE du Conseil du 12 juillet 1999 relative à la limitation de l'exposition du public aux champs électromagnétiques (de 0 Hz à 300 GHz), *J.O.C.E.*, L 199, 30 juillet 1999.

Question 3.4.

A plusieurs reprises, des contestations[79] ont vu le jour au sujet de l'indépendance de l'IBPT dans l'exercice de ses missions, au regard des exigences posées par le cadre règlementaire européen des communications électroniques. Contestations auxquelles l'Organisation de Coopération et de Développement Economiques (ci-après, OCDE) fait écho en 2009. L'OCDE estimait que suite à la réforme opérée en 2003[80] et relative au statut de l'IBPT, «il subsiste certaines interrogations quant à son indépendance : les membres du Conseil (organisme délibérant), notamment le président, sont nommés et peuvent être révoqués sur proposition de l'exécutif. Une incertitude demeure quant à la possibilité pour le gouvernement de casser les décisions de l'IBPT et à l'influence politique pesant sur les priorités des régulateurs»[81].

De plus, le même document précise: «bien que l'indépendance de l'IBPT ait été accrue en 2003, des signes montrent qu'il faudrait peut-être encore la renforcer, compte tenu de la participation de contrôle de l'État dans l'opérateur historique [...]. De ce fait, Belgacom contribue de façon significative au budget fédéral, d'où un possible conflit d'intérêt : l'État est un régulateur chargé de promouvoir la concurrence, mais par ailleurs il bénéficie des recettes de l'opérateur historique. En conséquence, la privatisation de Belgacom clarifierait davantage les incitations à donner davantage de pouvoirs au régulateur sectoriel. Au cours des années passées, un certain nombre de sources ont accusé le régulateur d'être soumis aux influences politiques (Platform, 2007, ECTA, 2008, Test-Achats, 2007, 2008) et de négliger la mise en œuvre du dégroupage de la boucle locale (Platform, 2007)»[82].

La loi du 18 mai 2009, portant des dispositions diverses en matière de communications électroniques[83], a permis de partiellement circonvenir aux problématiques pointées; cette législation comprenant des mesures modifiant le statut de l'IBPT et visant à simplifier la procédure d'imposition d'amendes, à majorer ces dernières, et à doter l'IBPT de plus de pouvoirs d'intervention sur le marché.

[79] Voy. notamment la question écrite de G. Deprez n° E-2610/06 du 14 juin 2016 se référant aux critiques de la Commission européenne dans son 11e rapport sur la mise en œuvre des directives européennes en matière de communications électroniques (février 2006). La question et la réponse de Mme Reding sont disponibles à l'adresse http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2006-2610&language=FR.

[80] Loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, *M.B.*, 24 janvier 2003.

[81] OCDE, *Études économiques de l'OCDE : Belgique*, juillet 2009, p. 136, disponible à l'adresse http://www.oecd-ilibrary.org/economics/etudes-economiques-de-l-ocde-belgique-2009_eco_surveys-bel-2009-fr.

[82] *Ibidem*, p. 146.

[83] Loi du 18 mai 2009 portant des dispositions diverses en matière de communications électroniques, *M.B.*, 4 juin 2009.

Cette intervention législative ne fut cependant pas suffisante aux yeux de la Commission européenne, qui initia en 2014 un recours en manquement contre l'état belge, considérant que «la législation belge ne garantit pas l'indépendance du régulateur national dans le domaine des télécommunications. En vertu des règles de l'UE dans ce domaine, les autorités réglementaires nationales responsables de la régulation du marché et du règlement des litiges entre entreprises doivent, en effet, agir en toute indépendance et ne solliciter ni accepter d'instruction en appliquant ces règles»[84], alors que «[l]a législation belge prévoit que le conseil des ministres belge peut, dans certaines circonstances, suspendre les décisions du régulateur des télécommunications belge, l'Institut belge des services postaux et des télécommunications (IBPT). En outre, la stratégie pluriannuelle de l'Institut est soumise à l'approbation du conseil des ministres belge»[85].

En réaction, la Belgique adopta une nouvelle loi[86] prévoyant que les «ministres de tutelle s'occupant de la réglementation sur les télécoms ne peuvent plus influencer le Conseil de l'IBPT en lui transmettant leurs objectifs prioritaires à mener dans ces secteurs. De plus, le régulateur n'a plus besoin de présenter son plan de projet stratégique au Conseil des ministres»[87].

Cette modification législative mit fin à la procédure initiée par la Commission à l'encontre de la Belgique, de telle sorte que la question de l'indépendance de l'IBPT n'a donc jamais reçu de réponse juridictionnelle, les adaptations successives de la législation relative à cet institut ayant *in fine* permis de clore la problématique.

4. Données dans l'économie numérique

Question 4.1.

La loi du 3 décembre 2017 portant création de l'Autorité de protection des données a été publiée au Moniteur belge le 10 janvier 2018. Cette loi réforme substantiellement la Commission de la protection de la vie privée. Cette dernière est rebaptisée « autorité de protection des données » et structurée en six organes composés de professionnels de la protection des données (un comité de direction, un secrétariat général, un service de première ligne, un centre de connaissance,

[84] Commission européenne, Communiqué de presse: *Télécommunications: la Commission poursuit la Belgique devant la Cour de justice de l'UE pour défaut d'indépendance de son régulateur national*, 16 octbre 2014, disponible à l'adresse http://europa.eu/rapid/press-release_IP-14-1145_fr.htm.

[85] Ibidem.

[86] Loi du 16 mars 2015 portant modification de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, *M.B.*, 7 avril 2015.

[87] M. Lepage, *Tout savoir sur l'IBPT, le régulateur belge des télécoms*, 20 novembre 2015, mis à jour le 11 mai 2017, disponible à l'adresse https://www.killmybill.be/fr/ibpt-regulateur-telecom-belge/.

un service d'inspection, une chambre contentieuse et un conseil de réflexion)[88]. L'indépendance des membres est renforcée, ceux-ci étant nommés par la Chambre des représentants sur la base de candidatures proposées, sans intervention du Conseil des ministres[89]. Les comités sectoriels, chargés jusqu'ici de contrôler les échanges de données entre les administrations sont supprimés. L'autorité de protection des données disposera du pouvoir d'amende, ce qui n'était pas le cas de la Commission de la protection de la vie privée[90].

Une loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel est en cours de rédaction. Le but de cette loi est d'organiser la mise en application du RGPD dans le système juridique belge, en tenant compte des particularités de ce dernier. Il s'agira notamment d'organiser, en Belgique, les traitements de données à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire ; le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques; le contrôle des échanges de données dans le secteur public, jusqu'ici effectué par les comités sectoriels, etc. ainsi que de transposer en droit belge la directive relative aux traitements de données effectués par les autorités judiciaires, policières et les services de renseignement et de sécurité.

Question 4.2.

Avant de répondre à cette question, il est important de garder en tête que la réglementation relative à la protection des données à caractère personnel reste à l'heure actuelle une législation assez méconnue des entreprises et plus particulièrement des PME, disposant généralement de moins d'accompagnement sur le plan juridique.

Même si les choses vont sans doute évoluer avec la future entrée en application du RGPD, il reste à craindre qu'un certain nombre d'entreprises belges n'aient pas encore entendu parler de ce texte, ou du moins ne réalisent pas encore qu'elles y seront soumises et ne mesurent pas le travail de mise en conformité nécessaire[91]. Ces dernières n'ont donc logiquement pas encore entamé de processus de mise en conformité.

[88] Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, article 7.

[89] Ibidem, article 39.

[90] Ibidem, article 100.

[91] Cette perception des choses est notamment corroborée par une étude récente de KaspersSky qui a interrogé des responsables IT en Europe, voyez: https://www.kaspersky.fr/blog/gdpr-poll/8817/
Ces résultats ne considérant que les entreprises disposant d'un département IT, il est probable que ces chiffres différeraient si l'ensemble des entreprises étaient cette fois interrogées.

Pour les entreprises qui souhaitent se mettre en conformité, il faut distinguer les entreprises qui respectaient l'ancien cadre légal des autres.

Les premières devraient s'adapter relativement bien aux nouvelles exigences du RGPD même si cela risque de leur demander un travail conséquent qui nécessitera du temps vu la taille de certaines entreprises et la complexité des différents processus utilisés.

Les secondes, qui découvrent la législation relative à la protection des données et démarrent donc de plus loin voire de zéro, ont beaucoup plus de mal à s'adapter et le RGPD devient pour elles un défi difficile à relever, surtout pour les petites entreprises qui n'ont souvent ni les connaissances, ni les ressources nécessaires.

Vu l'ampleur du travail et les délais relativement courts, il leur est conseillé de prioriser les différentes actions à mener et notamment commencer par dresser un inventaire des données à caractère personnel traitées[92].

A côté du travail de sensibilisation et d'accompagnement qui est effectué par la Commission de la Protection de la Vie Privée, certaines organisations professionnelles organisent à destination de leurs membres des formations sur le RGPD et développent à leur intention des outils de mise en conformité[93].

Question 4.3.

En matière de données générées par machine, la Belgique n'a, pour l'heure, pas encore creusé les pistes de réflexion lancées par la Commission européenne dans sa communication « Building a European Data Economy »[94], relatives, entre autres, à la libre circulation, à la portabilité, à l'accès, au transfert et à la propriété des données. Tout au plus peut-on dire que, au niveau belge, la question de la « propriété » des données s'avère problématique, dès lors que le régime de la propriété mis en place par le Code civil belge (Arts. 544 et s.) s'accommode mal du caractère incorporel des données. Dans ce contexte, certaines voix invitent à repenser ce régime classique[95], au vu des évolutions technologiques récentes, et de la valeur économique indéniable des données (générées par machine). Notons, à cet égard, que l'avant-projet de loi réformant le droit des biens dans le

[92] Pour le plan en 13 étapes proposé par la Commission de la Protection de la Vie Privée voyez: https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20FR%20-%20V2.pdf.

[93] A titre d'exemple voyez l'outils développé par AGORIA: https://www.agoria.be/fr/GDPR-Compass-votre-outil-Agoria-pour-une-conformite-au-GDPR-sans-souci

[94] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité européen des régions, "*Building a European Data Econo*my", Bruxelles, 10 janvier 2017, COM(2017) 9 final.

[95] P. Lecocq, *L'incorporel et le droit des biens: quo vadis?*, présentation réalisée dans le cadre de la Chair Francqui à la KU Leuven, en date du 16 novembre 2017.

Code civil belge s'intéresse «*aux aspects de statut réel des biens incorporels*»[96] et qu'il ranime le débat sur «*la question de savoir si les biens incorporels peuvent être l'objet d'une propriété*»[97].

Par ailleurs, la Commission européenne a invité les Etats membres à se montrer particulièrement attentifs au développement des véhicules autonomes[98]. Ce faisant, le Service public fédéral Mobilité et Transports a adopté un Code de bonnes pratiques d'expérimentation de véhicule autonomes en Belgique[99]. Ce dernier contient notamment des exigences relatives à la responsabilité de la sécurité de l'expérimentation, à la cyber-sécurité, ainsi qu'à l'enregistrement et la protection des données.

En matière d'Internet des Objets et de villes intelligentes, le débat n'est, pour l'heure, guère plus avancé. Ceci malgré un investissement croissant des entrepreneurs dans des projets estampillés « Smart City » ou « IoT », et les nombreuses problématiques qu'ils soulèvent, qu'il s'agisse des risques potentiels d'atteinte à la vie privée, des menaces pour la sécurité, ou des questions liées à la responsabilité.

Question 4.4.

Le droit au déréférencement, déduit des droits d'opposition et de rectification, lesquels étaient déjà énoncés dans la loi du 8 décembre 1992, n'a pas fait l'objet d'une consécration particulière en Belgique.

Depuis le prononcé de l'arrêt de la Cour de Justice, il existe des demandes de médiation devant la Commission de la protection de la vie privée lorsque Google se refuse à déréférencer certains liens[100].

Aucun cas ne semble avoir été porté devant les cours et tribunaux s'agissant du droit au déréférencement opposable aux moteurs de recherche.

La Cour de cassation de Belgique a cependant rendu un arrêt le 29 avril 2016 qui confirme l'existence d'un droit à l'oubli opposable aux sites éditoriaux de presse en ligne[101].

[96] Commission de réforme du droit des biens, *Avant-projet de loi portant insertion du Livre II « Droit des biens » dans le nouveau Code civil – Exposé des motifs*, 7 décembre 2017, disponible sur https://justice.belgium.be/sites/default/files/expose_des_motifs-_le_droit_des_biens.pdf, p. 6.

[97] Ibid., p. 155.

[98] Communication de la Commission, "*Building a European Data Econo*my", *op.cit*., p. 17.

[99] Service Public Fédéral Mobilité et Transports, *Véhicules autonomes: Code de bonnes pratiques d'expérimentation en Belgique*, septembre 2016, disponible à l'adresse https://mobilit.belgium.be/sites/default/files/resources/files/code_of_practice_fr_2016_09.pdf.

[100] Commission de la Protection de la Vie Privée (ci-après CPVP), *Rapport annuel 2014*, 2015, juin 2015, p. 43, disponible à l'adresse https://www.privacycommission.be/sites/privacycommission/files/documents/Rapport%20annuel%202014.pdf.

[101] Cass., 29 avril 2016, C.15.0052.F, disponible à l'adresse http://jure.juridat.just.fgov.be/view_decision.html?justel=F-20160429-1&idxc_id=302344&lang=FR.

Dans cette affaire, la Cour de cassation a rejeté le pourvoi introduit contre un arrêt de la Cour d'appel de Liège qui avait considéré que l'éditeur qui, après notification d'une personne physique, s'était abstenu de rendre anonymes certains articles de presse portant sur le passé judiciaire de cette dernière, pouvait, dans certaines circonstances, engager sa responsabilité extracontractuelle. Dans le cadre de cette affaire, le fait que les moteurs de recherche aient également pu participer à la production du dommage de la personne visée n'a pas été considéré comme une circonstance de nature à exclure la responsabilité du site éditorial.

CROATIA

Melita Carević*
Marko Jurić**

1. Internal Market and electronic commerce: Internet and e-commerce
1.1. Electronic Commerce, liability of Internet intermediaries

Question 1.1.1.
Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (hereinafter: "Directive on Electronic Commerce") has been transposed in the Croatian legal order through the Electronic Commerce Act (Official Gazette 173/2003, 67/2998, 130/2011, 36/2009, 30/2014). The first version of the Act already relied heavily on the legal solutions from the Directive on Electronic Commerce, despite the fact that at the time Croatia was not yet a member of the European Union. The Act has subsequently been amended several times in order for the complete transposition of the Directive on Electronic Commerce to be achieved. As far as can be seen from the preparatory documents[1], no specific legislative difficulties regarding the concept of intermediary service providers have been encountered during the transposition process. Regarding its application, as far as it was identified for the purposes of this research, there is currently no national case-law on the concept of intermediary service providers.

* Dr. sc. Melita Carević, LL.M., Assistant Professor at the Department of European Public Law, University of Zagreb – Faculty of Law.
** Dr. sc. Marko Jurić, Assistant Professor at the Department of Legal Informatics, University of Zagreb – Faculty of Law.
[1] Ministarstvo gospodarstva, rada i poduzetništva, Nacrt prijedloga Zakona o izmjeni Zakon o elektroničkoj trgovini, s konačnim prijedlogom zakona, Zagreb, veljača 2009., page 13, https://vlada.gov.hr/UserDocsImages//Sjednice/Arhiva//71_05.pdf (visited on 5 September 2017).

However, one remark should be made when it comes to the transposition of Article 14 of the Directive on Electronic Commerce – Article 18 of the Croatian Electronic Commerce Act unnecessarily narrows the grounds for liability exclusion contained in Article 14 paragraph 1 point a) of the Directive and contains an error in one of the grounds. The corresponding Article 18 paragraph 1 of the Croatian Electronic Commerce Act is worded as follows:

> "Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: – the provider does not have or could not have had actual knowledge of illegal activity of the recipient or of the content of information, and on court procedures on compensation of damages that would arise from the illicit activity of the user or from the content of the data stored, and if he was not aware and could not be aware of the facts or circumstances which would have made the illicit activity of the user apparent, ... "

Article 14 of the Electronic Commerce Act constitutes an incorrect transposition of the corresponding provision of the Directive because it requires that the information society service provider "could not have had" knowledge of illegal activity of information, which is not required by the Directive and is hard to prove in practice, and what is more, risks running dangerously close to the prohibition of a general monitoring obligation of the service provider. In any case, this requirement constitutes an unauthorised narrowing of the rule on the exclusion of liability of the information society service provider, which has been harmonised by the Directive, and therefore represents a breach of EU law. Furthermore, when it comes to the ground relating to court proceedings, the Croatian provision contains a mistake in describing this ground, since it puts it in the same category as actual knowledge on illegal activities or information.[2]

Finally, it should be noted that the Croatian Electronic Commerce Act prescribes one additional ground for excluding the liability of an information society service provider, which is not envisaged by the Directive, and that is granting access to third party data through linking.

[2] Regarding the question whether an intermediary service provider could have been aware of facts or circumstances from which the illegal activity is apparent, the Court applies the test whether "a diligent economic operator should have identified the illegality in question and acted in accordance with Article 14(1(b) of Directive 2000/31 (Case C-324/09, L'Oréal SA and Others v eBay International AG and Others, p. 120).

Question 1.1.2.

In L'Oréal v eBay the Court has applied the neutrality test, which focuses on the question whether the intermediary service provider conducts "merely technical and automatic processing of the data provided by its customers" or "plays an active role of such a kind as to give it knowledge of, or control over, those data"[3]. The Court ruled that if eBay "provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position"[4]. According to the Court's case-law, the essence of the test thus comes to knowledge of, or control over the relevant data and is anchored in recital 42 of Directive 2000/31.

In his opinion in L'Oréal v eBay, Advocate General Jääskinen considered the neutrality test to be inappropriate for cases of data hosting, provided by operators such as Google and eBay[5]. The main reason behind Advocate General's critique of the neutrality test is that it narrows down the cases in which a provider of a hosting service can rely on the liability exemption and that this can jeopardize the attainment of the Directive's objectives.[6] The Advocate General bases this conclusion on the claim that recital 42 of the Directive, and therefore the neutrality requirement, relates only to the exemptions listed in Articles 12 and 13, that is, exemptions for services consisting in "mere conduit" and "caching".[7]

Indeed, when looking at the system of liability exemptions under the Directive as a whole, one must admit that the application of the neutrality requirement to the liability exemption for hosting services is far from obvious. While Article 12 of the Directive, prescribing the liability exemption for services consisting in "mere conduit", and Article 13, a corresponding provision for caching services, explicitly require neutrality of the service provider by making it mandatory that the provider does not modify or select (Article 12) nor modify (Article 13) the information, Article 14 which relates to hosting does not prescribe such a requirement. When it comes to Article 14, the Court applied the neutrality criterion as an ancillary tool for determining whether the conditions from paragraph 1 point a) are fulfilled, or in other words, whether the provider had "actual knowledge of illegal activity or information", or in case of claims for damages, whether it was "aware of facts or circumstances from which the illegal activity or information is apparent". However, it must be emphasized that pursuant to Article 14 paragraph 1 point b), even if the provider knew about the illegal activity or information, it

[3] Case C-324/09, L'Oréal SA and Others v eBay International AG and Others, p. 113.
[4] Ibid., p 116.
[5] Opinion of AG in C-324/09, L'Oréal v eBay, p. 146.
[6] Ibid., p. 142.
[7] Ibid., p. 140-142.

will still not be held liable if it, "upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information".

While sounding pretty straightforward on paper, the neutrality requirement has faced difficulties when being applied in practice. Which action makes a provider undoubtedly know about the illegal activity or information? Is eBay obliged to investigate the legality of every piece of data it intervenes with, such as when optimizing the presentation of the offer for sale of one of its clients? Or would this be contrary to the prohibition of a general obligation to monitor, prescribed in Article 15 of the Directive? In order to stay on the safe side and not to engage in financially burdensome checks, the current stance taken by the Court incentivizes the providers of hosting services to always remain neutral in respect of data they host, which is not necessarily beneficial to the consumers.

The fact that the neutrality criterion might not have been consistently applied can be seen from the Court's ruling in Google France, where the Court found that Google remained neutral when providing its paid referencing service.[8] The Court stated that "the role played [...] [by a] service provider is neutral, [...] [if] its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores"[9] Despite the fact that it is hard to question the positive outcome of the Google France case, it remains questionable whether Google must have known about the activity and information in question, since it had received a payment regarding that precise activity. This only shows how blurred the lines of the current test are when faced with the complex mixture of tasks performed by hosting service providers. Finally, it should be noted that when in doubt whether an hosting service provider is "neutral" regarding certain content, it suffices to send a notice of the illegality of the content at issue in order for the hosting service provider's obligation to expeditiously remove that content to be triggered.

Question 1.1.3.

The current regime of notice-and-take down under the Directive on Electronic Commerce puts information society service providers in a rather unenvious position. In theory, upon receiving a notice on the illegal content which is being hosted, a hosting service provider should perform a complex task of balancing the conflicting rights which are at stake in order to decide whether the reported content should be removed. The more complex the content of the conflicting rights, the harder it is for an information society service provider to make that

[8] Case C-236/08 to C-238/08, Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08), p. 116.
[9] Ibid., p. 114.

decision. In practice, internet service providers are not well-placed to resolve such complex legal questions, especially given the fact that if they make the wrong call, they could lose the protection of the liability exemption under Article 14 of the Directive on Electronic Commerce. As pointed out by numerous authors, this has led to a paradoxical situation in which internet service providers have a strong incentive to remove all the reported content, without engaging into the merits of the claim for illegality of that content, which would require time, legal and financial resources.[10] It can therefore be concluded that the current notice-and-takedown regime is not appropriate for all kinds of infringements, ranging from intellectual property rights, free speech and criminal offences, such as child pornography.

One of the solutions to this problem which has been suggested in the literature is to establish different types of notice-and-action procedures for different types of infringing content.[11] Angelopoulos and Smet consider that the gravity of the reaction to the infringing content should depend on the seriousness of a fundamental right's violation[12] Studying different legislative solutions which are already in place in some jurisdictions, they suggest a notice-and-notice procedure for copyright infringements.[13] Instead of immediately having to take down the allegedly infringing content, an internet service provider would only be obliged to "forward the notice to the indicated end-user", who would be free to choose whether to remove the content at issue, or respond to the copyright claim.[14] In case no agreement is reached between the parties, they would have the option of initiating formal proceedings.[15] Regarding defamation claims, the same authors suggest a notice-wait-and-takedown procedure, according to which the internet service provider would forward the notice to the content provider and wait a certain period of time before taking further action.[16] Depending on the response the internet service provider receives, it would be better-placed to decide whether or not to remove the problematic content.[17] A special procedure is furthermore for hate speech – for this type of infringement the author sug-

[10] Christian Ahlert, Chris Marsden, Chester Yung, How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation page 10-11, http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf (visited on 10 September 2017).

[11] Christina Angelopoulos, Stijn Smet, Notice-and-fair-balance: how to reach a compromise between fundamental rights in European intermediary liability, Journal of Media Law, 2016, Vol 8. No. 2., 266-301, p. 292.

[12] Ibid., p. 292.

[13] Ibid., p. 294, 295.

[14] Ibid., p. 295.

[15] Ibid., p. 295.

[16] Ibid., p. 296.

[17] Ibid., p. 296.

gest a more straightforward response – the current notice-and-takedown and the notice-and suspension procedure as an additional option.[18] Finally, for the most severe violations of absolute fundamental rights, such as cases of child pornography, the authors advocate an automatic takedown procedure, and a notice-and-stay-down as a backup option.[19]

Similarly, a special solution for some cases, such as copyright infringements, has also been described by Leersen[20], who relays on the information given in a Commission Staff Working Document on Online services, including e-commerce, in the Single Market. One of the main problems with the current regime is high likelihood that a notice will result in the removal of the reported content, even though the hosted content is perfectly legal. [21]. In order to ensure that the current notice-and-takedown system cannot be so easily abused, it has been suggested that the party who submits unfounded copyright notices is to be held liable for the damages caused by wrongful removal of legal content.[22]

A characteristic which most of the solutions which have so far been put forward have in common is that they will no longer result in a speedy removal of the allegedly infringing content, which has so far been possible only in an online environment (apart from obvious and most severe infringements). They will therefore no longer offer almost absolute protection which in practice has been given to the party alleging a violation of his/her right, which is surely a step in a positive direction.

Question 1.1.4.

By the time of writing this report, the authors have not identified any judgments dealing with injunctions under the Directive on Electronic Commerce in Croatia. However, a request for an injunction seems to be raised in a case between the Croatian Performers' Rights Collecting Society versus Croatian Telecom and Deezer, which is currently being decided in first instance before the Commercial Court in Zagreb.

[18] Ibid., p. 297, 299.

[19] Ibid., p. 292.

[20] Patrick Leersen, The Limits of Limited Liability under Article 14 of the E-Commerce Directive – How 'Notice and Takedown' sidelines the use of copyright exemptions, Maastricht Student Law Review (2014)1, p. 13, http://www.mslawreview.eu/wp-content/uploads/2014/12/Leersen.pdf (visited on 10 September 2017).

[21] Commission Staff Working Document, Online services, including e-commerce, in the Single Market (COM(2011) 942 final, of 11.1.2012., p. 45.

[22] Patrick Leersen, The Limits of Limited Liability under Article 14 of the E-Commerce Directive – How 'Notice and Takedown' sidelines the use of copyright exemptions, Maastricht Student Law Review (2014)1, p. 13, http://www.mslawreview.eu/wp-content/uploads/2014/12/Leersen.pdf (visited on 10 September 2017).

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.
As far as this research has identified, there were no particular difficulties in the transposition of remedies under Directive 1999/44/EC into the Croatian legal system, nor their application.

Question 1.2.2.
Since this area has not been previously targeted by legislation at the EU level, the proposed Directive on certain aspects concerning contracts for the supply of digital content certainly represents an important step towards the protection of consumer rights when purchasing digital content. The level of harmonisation targeted by the proposal is maximum harmonisation, which excludes more or less stringent national provisions and thus eliminates potential obstacles to the creation of a digital single market. However, despite having numerous positive effects on the trade in digital content, the proposed Directive seems to leave room for further improvement.[23]

Question 1.2.3.
The proposed Directive on certain aspects concerning contracts for the online and other distance sales of goods certainly contributes to the achievement of a digital single market, because it eliminates some of the key uncertainties that both sellers and consumers are currently facing when engaging in online trade. By harmonising some of the key contractual rights, such as consumer's remedies for the lack of conformity with the contract, and clarifying some of the current provisions of the Consumer Sales Directive[24], the proposal is highly likely to have a positive impact on seller and consumer confidence, two of the factors which have so far hampered the development of online cross-border trade. However, the proposal has at the same faced criticism for creating fragmentation of the consumer protection regime.[25]

[23] For an in-depth analysis of the proposal and its critique see Vanessa Mak, The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content – Workshop for the Juri Committee on Legal Affairs of the European Parliament, New rules for contracts in the digital environment, 2016, pp. 1-28, p. 4. http://www.epgencms.europarl.europa.eu/cmsdata/upload/a6bdaf0a--d4cf-4c30-a7e8-31f33c72c0a8/pe__536.494_en.pdf (visited on 10 September 2017).
[24] For an overview of some of the main elements of the proposal, see Rosa Milà Rafel, "The Directive Proposals on Online Sales and Supply of Digital Content (Part II): conformity and remedies for lack of conformity". IDP. Revista de Internet, Derecho y Política. (2016) 24, pp. 50-63.
[25] Jan Smits, The new proposal for harmonised rules for the online sales of tangible goods: conformity, lack of conformity and remedies". Workshop for the Juri Committee on Legal Affairs of the European

Question 1.2.4.
The harmonisation of consumer protection rules stemming from the proposed Directives on the supply of digital content and online sale of goods might have a twofold effect on the enforcement of EU consumer protection legislation. On one hand, the harmonized rules are likely to facilitate Member State cooperation on their enforcement. However, on the other hand, the fragmentation of consumer protection rules caused by different sets of rules for online and offline purchases might lead to difficulties in their enforcement, both within a single Member State, and in different Member States. In any case, the harmonisation brought by the proposed Directives will increase the overall level of consumer protection within the Union, but since the proposed Directives will lead to maximum harmonisation it will at the same time necessarily lower the existing levels of protection in some Member States.[26]

Question 1.2.6.
As far as this research has identified, having consulted the relevant stakeholders and performed the search of available case-law, so far there have not been any actions on the basis of consumer law against online provider's terms and conditions before Croatian courts.

1.3. Geo-blocking

Question 1.3.1.
Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters can be considered as *lex generalis* in relation to the proposed Regulation on geo-blocking, in matters of determining jurisdiction. However, Article 1 point 5 of the proposed Regulation on geo-blocking explicitly states that it "shall not affect acts of Union law concerning judicial cooperation in civil matters. Compliance with this Regulation shall not be construed as implying that a trader directs his or her activities to the Member State where the consumer has the habitual residence or domicile within the meaning of point (b) of Article 6(1) of Regulation (EC) No 593/2008 and point

Parliament, New rules for contracts in the digital environment, http://www.epgencms.europarl.europa.eu/cmsdata/upload/3f55190a-e9dc-43f0-a977-b7ee0e824485/pe_536.492_en_print.pdf (visited on 10 September 2017).

[26] Jan Smits, The new proposal for harmonised rules for the online sales of tangible goods: conformity, lack of conformity and remedies". Workshop for the Juri Committee on Legal Affairs of the European Parliament, New rules for contracts in the digital environment, p. 16., http://www.epgencms.europarl.europa.eu/cmsdata/upload/3f55190a-e9dc-43f0-a977-b7ee0e824485/pe_536.492_en_print.pdf (visited on 10 September 2017).

(c) of Article 17(1) of Regulation (EU) 1215/2012"[27]. It can therefore be concluded that the proposed Regulation on Geo-blocking will not enable the buyer in one Member State to rely on the provisions for determining jurisdiction for consumer contracts under Regulation 1215/2012, if the criterion of "directing activities to another Member State where the consumer has its domicile" is the only provision that the buyer can rely on.

1.4. Questions related to the collaborative economy

Question 1.4.1.

The most contentious legal issue by far which has so far been raised in Croatia in the context of collaborative economy is the operation of Uber Croatia. Ever since Uber entered the Croatian market in 2015 it has been operating in an unregulated environment, providing transport services through its platform, but not complying with all the requirements for the provision of taxi services, prescribed by the Road Transport Act (Official Gazette 82/13). Under the currently applicable regulation of taxi services, the operation of Uber would be practically impossible, because it would have to obtain special taxi licenses for each of its vehicles, the number of which is strictly limited and awarded on the basis of the decisions of local governments. Furthermore, in order to satisfy the requirements of the Road Transport Act, Uber would have to comply with a number of special, fairly restrictive provisions, such as to charge its users the price determined by a taximeter and require its drivers to pass a number of tests, such as the test of knowledge of local landmarks. Despite generally being welcomed by the citizens, Uber has been faced with strong disapproval from the taxi companies and the Croatian Chamber of Commerce. On several occasions Uber drivers have even been physically attacked[28] and taxi drivers have so far organized several protests against Uber[29]. The Ministry of Maritime Affairs, Transport and Infrastructure, which considers Uber illegal, has filed an action for the prohibition of Uber's activities before the Misdemeanour Court in Zagreb. The first instance decision in favour of Uber has been adopted in September 2017.[30]

[27] European Commission, Proposal for a Regulation of The European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC, COM(2016) 289 final, 25.5.2016, page 17.

[28] https://dnevnik.hr/vijesti/hrvatska/novi-napad-taksista-deset-vozaca-ubera-napadnuto-u-zadru-u-proteklih-tjedan-dana---481134.html (visited on 25 September 2017).

[29] https://www.vecernji.hr/vijesti/dubrovnik-taksisti-prosvjed-uber-jadranska-magistrala-1185250 (visited on 25 September 2017).

[30] http://www.novilist.hr/Vijesti/Hrvatska/Sud-odbio-Butkovica-nema-zabrane-aplikacije-Uber (visited on 7 October 2017).

A similar action against Uber has also been filed by the Croatian Chamber of Commerce before the Commercial Court in Zagreb, however at the time of writing this report no decision has yet been reached.[31] By the end of July 2017, the inspection of the Ministry of Maritime Affairs, Transport and Infrastructure has handed out fines in the amount of 7 million kunas to Uber's drivers and has confiscated 18 cars.[32] Interestingly, the Ministry of Economy, Entrepreneurship and Crafts has taken a more favourable stance towards Uber, which it considers to be an information society service provider, and therefore advocates a more flexible approach towards the provision of its services.[33]

At the time of writing this report, amendments to the Road Transport Act are being drafted. Partial liberalization of the taxi services has been unofficially announced, with more taxi licenses being granted, which would create an opportunity for Uber drivers to legally operate on the market, and certain minimum safety requirements will be prescribed, which will have to be respected by all taxi service providers.[34]

Unlike the UberX service, Uber Boat has not caused a similar uproar when entering the Croatian market in June 2017, due to a less restrictive set of rules applicable to boat transport services, which Uber Boat complied with.[35]

Another major collaborative economy business which operates on the Croatian market is Airbnb, but its presence has so far not attracted such strong public attention. Finally, it should be noted that the need for further liberalization of the provision of collaborative economy services in Croatia has been pointed out by the European Commission in its 2017 Country Report on Croatia.[36]

Question 1.4.2.

Traditional service providers, such as providers of taxi services[37] and tourist accommodation services have often raised issues of unfair competition stem-

[31] https://www.hok.hr/press/objave_za_medije/hrvatska_obrtnicka_komora_podigla_tuzbu_protiv_ubera_zbog_poticanja_na_nelegalni_prijevoz_putnika (visited on 25 September 2017).

[32] https://www.vecernji.hr/vijesti/dubrovnik-taksisti-prosvjed-uber-jadranska-magistrala-1185250 (visited on 25 September 2017).

[33] http://www.poslovni.hr/hrvatska/ministarstvo-gospodarstva-uber-treba-rijesiti-kroz-reformu-trzista-usluga-329815 (visited on 25 September 2017).

[34] https://www.vecernji.hr/vijesti/taksi-licencije-novi-zakon-o-prijevozu-u-cestovnom-prometu-uber-1187199 (visited on 25 September 2017).

[35] http://net.hr/danas/hrvatska/uberboat-sada-i-na-moru-nova-mogucnost-za-putovanje-do-otoka-ili-za-cjelodnevnu-avanturu/ (visited on 25 September 2017).

[36] Commission Staff Working Document, Country Report Croatia 2017 Including an In-Depth Review on the prevention and correction of macroeconomic imbalances, SWD(2017) 76 final, 22.2.2017 , page 44.

[37] https://www.tportal.hr/biznis/clanak/hok-tuzi-uber-krse-toliko-zakona-da-bi-mogli-napisati-knjigu-20170201 (visited on 25 September 2017); https://www.hok.hr/press/objave_za_medije/uber_nelojalna_konkurencija_taksi_prijevoznicima (visited on 7 October 2017).

ming from collaborative economy business that do not comply with the applicable legislative requirements and therefore do not bear the same financial burden as traditional service providers. It should be emphasised that even though this represents a competition problem for traditional service providers from the economic perspective, it does not raise competition law issues, but rather questions of efficient enforcement of laws applicable to traditional service providers, and from the policy perspective, the need for those laws to be liberalised. Nevertheless, competition law issues might arise from the other side of the coin, regarding barriers to entry to the market of traditional services.

Question 1.4.3.
So far no specific legislation has been enacted in respect of services active in the collaborative economy. Providers of those services are therefore currently left with a choice to either obtain all the necessary authorisations which are required for corresponding traditional services, such as taxi services, or apartment rental services, or to operate in an unregulated area. While Uber Croatia currently requires all drivers to be registered and to have a minimum guarantee of their driving skills, as mentioned above in the answer to Q1 1.4.1., it does not comply with all the requirements for providing traditional taxi services (namely, its drivers do not have taxi licenses, the number of which is relatively low and strictly limited and do not pay various fees that traditional taxi drivers pay. However, Uber's drivers currently do comply with their tax obligations).

Airbnb is on the other hand faced with lower administrative burden, since the number of short-term apartment rentals is not regulated by law. In order for a provider of an Airbnb service to comply with Croatian laws, it has to register the fact that he/she is providing short-term renting of his/her apartment, pay a relatively small registration fee and comply with the prescribed tax obligations. While Airbnb itself does not control whether its users are registered with the national authorities in Croatia, it is generally known to be supportive to the authorities in order to prevent unregistered renting.[38]

Question 1.4.4.
Under the current legislative framework in Croatia, there are no specific rules on consumer protection regarding services provided by peer-to-peer platforms. Therefore, the same rules as in the offline world apply – in case the service provider is not registered for the provision of the service at issue, only the provisions of the Civil Obligations Act (Official Gazette 35/05, 41/08, 125/11, 78/15) can be

[38] http://www.netokracija.com/airbnb-sinisa-topalovic-horwath-htl-omgcommerce-118953 (visited on 25 September 2017).

triggered. On the other hand, in cases when the service provider is registered for the provision of a particular service, the Consumer Protection Act (Official Gazette 41/14, 110/15) is also applicable.

Question 1.4.5.
Pursuant to 4 Article of the Trade Act (Official Gazette 87/08, 96/08, 116/08, 76/09, 114/11, 68/13, 30/14), a trader is a natural or legal person registered for the sale and buying of goods and/or the provision of services in the course of trade. A provider of a peer-to-peer service would thus qualify as a trader if he/she would obtain the necessary registration.

However, the Consumer Protection Act lays down a wider definition of a trader in Article 5 point 26 for the purposes of application of that Act. According to this definition, a trader is any person who concludes a legal transaction or operates on the market within its commercial, business or professional activity or a craft, including a person which acts on behalf or on the account of a trader. The Consumer Protection Act therefore considers the providers of all services as trades, as long as they are operating within their commercial, business or professional activity or a craft.

Question 1.4.6.
Since their entry on the Croatian market, peer-to-peer services such as Uber and Airbnb do not seem to have suffered from the lack of consumer confidence. According to a Eurobarometer survey performed less than a year after Uber first started operating in Croatia, the public awareness and support for collaborative economy business seemed to be following the EU trends.[39] According to the data obtained from the Ministry of Economy, Entrepreneurship and Crafts, only one complaint regarding Uber's service has been submitted so far, regarding its promotional action and free rides, when due to the overload of the system one passenger was left without an already scheduled ride. It therefore seems that consumers so far do not seem to be concerned with the safety and reliability of services in the collaborative economy and that online rating and review system has served as a sufficient mechanism to ensure consumer confidence and information availability.

[39] European Commission (2016e), The use of collaborative platforms, Flash Eurobarometer 438, March 2016, available through https://data.europa.eu/euodp/data/dataset/S2112_438_ENG (visited on 25 September 2017).

2. Digital media

Question 2.1.
In the Croatian media landscape, traditional publishers are increasingly enhancing their online presence via portals which provide content in various forms, including text and audio-visual clips. This is particularly true in regard to several most prominent national publishers, which now routinely provide their own audio-visual content, either as an addition to textual articles or as a standalone news items. In such circumstances, issues which gave rise to recent CJEU's jurisprudence are probably likely to arise sooner or later. However, there have yet been no reported cases in the domestic practice. Similarly, there have set been no reported disputes concerning the application of the country-of-origin principle.

Legally speaking, definition of the "programme", prescribed in the Article 1(b) of the AVMSD, is implemented fully and without any differentiation in the Article 2(1)(4) of the Croatian Electronic Media Act (hereinafter: EMA). Therefore, EMA can and must be interpreted in line with the CJEU's jurisprudence, including the C-347/14 (*New Media Online GmbH v Bundeskommunikationssenat*) case.

Question 2.3.
By the time of writing this report, the authors have not identified any disputes of this kind.

Question 2.4.
Regulatory authorities in the field of electronic media in the Republic of Croatia are the Agency for Electronic Media and the Electronic Media Council. Agency for Electronic Media is an independent legal entity vested with public authority, and Electronic Media Council is its seven-member management board. Council's president and members are appointed for a five-year term by the Croatian Parliament, upon the proposal of the Government. They can be removed from the office only in cases explicitly stipulated in the law (EMA).

Speaking about political and/or commercial pressure on media regulators, there have been several prominent cases which have triggered debate on the national and even EU level. Most prominently, in 2016 Electronic Media Council decided (unanimously) to suspended operating license of *Z1* TV for three days, on the account that its programme contained an item which constituted hate speech and discrimination on the basis of religion.[40] This decision triggered significant public outcry from different sides of political spectrum and ultimately led to highly politicized public protests against the Agency for Electronic

[40] http://narodne-novine.nn.hr/clanci/sluzbeni/2016_01_10_262.html (visited on 30 September 2017).

Media and the Council. Several months later, the Government refused Council's annual report, but it failed to request its dismissal by the Parliament. This was interpreted by many media associations and NGOs as an undue political pressure against the independence of media regulator.[41] Simultaneously, Council's president submitted her resignation to the relevant minister and the government, but this was also not discussed by the Parliament for several months, due to breakdown of the coalition which formed the government.

Notwithstanding certain cases of undue political pressure which occurred in practice, we consider that the Croatian experience with the independence of Agency for Electronic Media and the Electronic Media Council is a positive one. If anything, looking from the perspective of a new Member State and with regard to experience of other independent regulators (i.e. in the field of personal data protection) we consider that introduction of specific independence requirements for media regulators at EU level would be a significant step forward. In any event, we cannot see any legal obstacles which would prevent introduction of such requirements on the national level.

Question 2.5.
In general, application of the rules against hate speech is very often contentious. In particular, this is associated with some country-specific cases of using slogans and insignia of past totalitarian regimes. Also, the role of the national public broadcasting company (Croatian Radiotelevision) is continuously contentious, in the context of its political neutrality, which is relevant due to its significant impact on national media scene. However, we believe that these issues should properly be addressed on the national level. In this context, it is not the further harmonization of the law which seems necessary. On the contrary, better enforcement of existing legal rules and further strengthening of independence of national regulators and broadcasting companies is the most important task.

Question 2.6.
By the time of writing this report, the authors have not identified any issues of this kind. In particular, Data Protection Agency has not been particularly active in applying data protection laws in the context of broadcasting activities.

[41] http://www.osce.org/fom/226861; http://www.fairpress.eu/blog/2016/03/30/chairman-of-csa-has-expressed-his-regret-because-of-mirjana-rakics-resignation-hnd-we-support-reactions-of-the-french-media-regulatory-authority-hnip-rakic-as-the-president-of-the-council-showed/; http://civic-forum.eu/en/civic-space/croatian-governments-triple-attack-on-autonomous-media-civil-society-and-culture (visited on 30 September 2017).

Question 2.7.
Yes. Pursuant to the Croatian Copyright and Related Rights Act (hereinafter: CRRA), broadcasting organizations have the exclusive right "to (1) rebroadcast its broadcasts by wire or wireless means; (2) to fix its broadcasts; (3) to reproduce its fixed broadcasts (4) to distribute its fixed broadcasts, except the rights of their rental and lending; (5) to publicly communicate its broadcasts if such communication is accessible to the public against payment of an admission; (6) to make available to the public of its fixed broadcasts.[42] However, by the time of writing this report, the authors have not identified any instances where these rules have been applied to online transmissions, although the provisions of the CRRA would not prevent such application.

3. Data in the digital economy

Question 3.1.
No such rules were present on the national level. Currently, there is no specific approach towards zero-rating. It is not explicitly regulated in the legislation, and to the best of our knowledge, national ISP's do not use such practices.

Question 3.3.
To the best of our knowledge, there are currently no legal challenges regarding spectrum management in Croatia.

Question 3.4.
The independence of the Croatian Regulatory Authority for Network Industries was put into question in 2012 when the Government enacted an amendment to the Electronic Communications Act (Official Gazette 133/2012), on the basis of which the number of members of the Council of the Agency was lowered from seven to five, for the purposes of more efficient governance. Even though the change in the composition of the Council was not problematic in itself, the aforementioned amendment to the Electronic Communications Act required that due to the change in the composition, all of the existing members of the Council had to be re-appointed.

4. Data in the digital economy

Question 4.1.
On the constitutional level, Republic of Croatia provides for a very strong protection of personal data. Croatia's Constitution from 1990 therefore provides

[42] Copyright and Related Rights Act (*Zakon o autorskom pravu i srodnim pravima*), Official Gazette, nos. 167/2003, 79/2007, 125/2011, 80/2011, 141/2013, 127/2014, 62/2017 (hereinafter: CRRA), Article 143.

explicit protection to personal data in its Article 37, which emphasizes duties of care and secrecy vis-à-vis such data, prohibits their use contrary to the purpose for which they have been collected and stipulates that personal data can only be processed on the basis of data subject's consent, or in accordance with the legislation. Unfortunately, it took more than one decade for the Croatian legislators to enact this legislation. It was not until 2003, when Croatian started to harmonize its legislation with the EU acquis, that Croatian parliament enacted specific act regulating processing of personal data. This was 2003 *Personal Data Protection Act* (PDPA), which is (with several amendments) still in force. In its scope and design, PDPA represents almost literary implementation of the *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. In the following years, sector-specific norms, covering protection of personal data in the field of electronic communications, police and criminal matters, banking sector and many others, were also enacted.

From a policy perspective, the main issue with regard to the personal data protection in Croatia stems from the fact that the relevant legal rules were more or less "imported" in the domestic legal framework. This is because personal data protection, although recognized on the constitutional level, did not enjoy significant prominence as a social value. Therefore, PDPA and other relevant statutes were enacted primarily in order to fulfil the necessary conditions in the process of the accession to the EU. In other words, in dealing with data protection law, Croatian legislators were motivated more by the need to satisfy certain external requirements, and less by the will to address relevant policy issues.

Currently, Croatian Ministry of Public Administration and the Personal Data Protection Agency are actively engaged in the drafting of new Personal Data Protection Act, which should come into force after GDPR starts applying. However, there are some drawbacks in this context. Most importantly, since the beginning of 2016 there have been several significant changes in the coalitions that formed two Croatian governments. This also had an impact on the legislative process, and as a result some important statutes, including the new PDPA, are being drafted more slowly than would ordinarily be the case. In any event, it can still be assumed that the new PDPA would be enacted in time, and that it will start applying in 2018.

New legislative framework for personal data protection will bring new challenges for the Data Protection Agency. Namely, since its establishment in 2003 this agency has mostly focused on the administrative and educational activities. On the other hand, only a limited number of misdemeanour and criminal proceedings in cases of violations of the PDPA have been initiated. This is likely to change after GDPR starts to apply. It is to be expected that Data Protection Agency will now have to put more emphasis on the enforcement activities, especially in the light of new powers envisaged in the GDPR.

Question 4.2.
From the market perspective, it is fair to say that the level of awareness regarding the compliance with the GDPR corresponds to the size of business operators. In general, large enterprises are actively preparing for the application of the GDPR and are taking steps to ensure compliance with it. On the other hand, small and medium size enterprises are less engaged. It is to be noted that the Data Protection Agency is currently very active in various educational activities with regard to the future legislative framework, and many entities from both the public and private sector are participating in these programs. Also, since the enactment of the GDPR many private consultancy services have been offered on the market. These are mostly provided by the companies specialized for data security and educational activities.

Moreover, there is also urgent need to address various issue of traffic data retention, in the light of last year's landmark CJEU's judgement in joined cases C-203/15 and C-698/15 (Tele2 and Watson). Currently, communication service providers operating on the Croatian market are still under obligation to retain traffic data, in accordance with the Electronic Communication Act (ECA). Provisions of this statute create a retention obligation which *de facto* corresponds completely to the one established on the basis of (now invalidated) EU Data Retention Directive. In the light of Tele2 and Watson, general and indiscriminate data retention obligation imposed on the basis of national legislation might impose impermissible restriction of the fundamental rights and freedoms (to personal data protection, privacy and freedom of expression). Although no decisions in this regard have been issued by the Croatian courts and other authorities, it is to be expected that the issue of data retention will have to be addressed in the near future.

Question 4.3.
By the time of writing this report, the authors are unable to report on any significant debate in relation to this topic in the national legal scholarship.

Question 4.4.
By the time of writing this report, the authors are unable to report on any significant developments in relation to the "right to be forgotten" on the national level. To be sure, there have been cases before the data protection authority where removal of personal data was requested. However, these cases have usually been solved by the application of general data protection rules. In particular, there was one prominent case concerning publication of personal data of government officials, pursuant to the Act on Prevention of the Conflict of Interest. In this case, Croatian Data Protection Agency ordered some personal data (marital status,

formal or informal cohabitation, number of children, ...) to be removed from the registry, on the account that these data were not relevant in the context of prevention of conflict of interest.[43]

[43] http://azop.hr/news/agency/resume-of-the-decision-of-the-croatian-data-protection-agency-legal-and-fac (visited on 30 September 2017).

CZECH REPUBLIC

Pavel Loutocký
Jakub Míšek
František Kasl

1. Internal Market and electronic commerce : Internet and e-commerce
1.1. Electronic Commerce, liability of Internet intermediaries

Question 1.1.1.

Liability limitations stipulated in the E-Commerce Directive were transposed into the Czech legal order by the Act No. 480/2004 Sb., on certain services of information society, as amended.

The biggest problem was that the legislator formulated hosting exception from the general liability for content as a new kind of liability and not as a "safe harbour". The provision reads as follows:

> "*Section 5*
> *Liability of the service provider for the storage of information provided by a user*
> *(1) A provider of a service that consists of the storage of information provided by a user, shall be responsible for the contents of the information stored at the request of a user only if he*
> *a) could, with regard to the subject of his activity and the circumstances and nature of the case, know that the contents of the information stored or action of the user are illegal; or*
> *b) having, in a provable manner, obtained knowledge of illegal nature of the information stored or illegal action of the user, failed to take, without delay, all measures, that could be required, to remove or disable access to such information.*
> *(2) A service provider referred to in paragraph 1 shall always be responsible for the contents of the information stored if he exerts, directly or indirectly, decisive influence on the user's activity.*"[1]

[1] Unofficial translation.

Similar wording is present also in the case of mere conduit (Section 3 of the Act). The problem with this wording is that it can be easily interpreted in the way that once the conditions of safe harbour are breached, the service provider is immediately liable for the content. However, that should not be (and according to the Directive is not) the case. Existence of safe harbour and actual liability are two questions which are to be considered separately.

Czech legal doctrine has already created an "euro-conformal" interpretation[2], which follows the logic of the Directive, and is generally acknowledged nowadays.

The second difference between Czech Act and the Directive is in the wording of Section 5, subsection 1 letter a) of the Act, which is the implementation of Art. 14, subsection 1, letter a) of the Directive No. 2000/31/EC. In a question whether the service provide has a "constructive knowledge", as Martin Husovec calls it[3], and thus cannot rely on the safe harbour exemption, it is necessary to evaluate, whether the service provider has knowledge about illegality of the content in the light of *a specific case and nature of the provider.*

There are only a few court decisions dealing with the question of ISP liability. In decisions of the *Prolux* case, in contrast with what we mentioned earlier, courts used the wrong interpretation of liability as a "new kind of liability based on the Act No. 480/2004 Sb.".[4]

Company Prolux Consulting Int. dealing in real estates, sued company Internet Info, an operator of a webpage mesec.cz. This page offers articles and news from the personal finance area. Under the articles there is a place for discussion of users. There was a discussion under an article named "*Do you want to sell an apartment: Alone, or with the estate agency?*"[5], in which several anonymous readers described their bad experience with Prolux as follows:[6] "*Prolux lies as a swine*", "*I have never thought that I am that stupid to trust such phoney*", or "*Hi, I am also a victim of caddish and mendacious company Prolux*". The company Prolux notified webpage operator about the discussion posts and demanded for the discussion to be taken down. However, Internet Info declined to do that because it did not see the claims as proven to be lies. Thus, Prolux sued Internet Info to remove disputed

[2] See e.g. in Czech: Martin Maisner "Zákon o některých službách informační společnosti. Komentář" [Act on Some Information Society Services. Commentary]. 1. vydání, Praha: C. H. Beck, 2016; in Slovak: Martin Husovec "Zodpovednosť na internete: podľa českého a slovenského práva" [Responsibility on the Internet: Under Czech and Slovak Law], Praha: CZ. NIC, 2014.

[3] See in Slovak: Martin Husovec "Zodpovednosť na internete: podľa českého a slovenského práva" [Responsibility on the Internet: Under Czech and Slovak Law], Praha: CZ. NIC, 2014, p. 108.

[4] The decisions of the Prolux case are as follows: decision of the City Court in Prague (the first instance) was from 17 March 2010, No. 10 Cm 47/2009-39; decision of the High Court in Prague (court of appeal) from 2 March 2011, No. 10 Cm 47/2009-39; and decision of the Supreme Court from 31 August 2013, No. 3 Cmo 197/2010.

[5] Unofficial translation.

[6] The translations are not precise word by word.

contributions and to pay satisfaction. City Court in Prague found Internet Info liable for the content and ordered it to remove the whole discussion from the web page. However, the court did not grant the satisfaction, with notion of "*controversial practices*" of Prolux.[7] Both parties to the case appealed. High Court in Prague dismissed appeal of Prolux, and partly approved appeal of Internet Info, when the decision was changed as follows: Internet Info is liable for the content and must therefore remove the sentence "*Prolux lies as a swine*" from the web page. The court reasoned existence of liability as based on the provision of the Act No. 480/2004 Sb. General provision concerning liability for defamation was considered, when the court was deciding whether the safe harbour rules were overcome. The Supreme Court confirmed decision of High Court in Prague.

The second case is *Parlamentni Listy*.[8] In this case the court found company Our Media (which runs internet news portal Parlamentní Listy) liable for discussion that was present under an article from 26 October 2011. The claimant considered the controversial discussion messages, which were aimed against him, to be racist, grossly insulting, violent to morbid, intolerant, ridiculous and totally deviating from the limits of generally accepted rules of decency in a democratic society. Defendant removed contested discussion on 9 March 2013. The court agreed with the claimant, and stated that such discussions are not covered by the freedom of speech. Then the court considered, whether the defendant can rely on the safe harbour, and decided that it is not the case, because the way, how defendant runs the service and encourages and moderates the discussions shows that it is the active hosting. Thus, the defendant was found liable in accordance with relevant provision of the Civil Code and was ordered to pay compensation.

The court in this case interpreted safe harbour and liability limitation correctly in the "euro-conformal" way. It can be mentioned that the court cited L'Oreal SA v eBay case in its argumentation.

Question 1.1.2.

The test for liability from the decision L'Oréal v eBay was not overly contested either in court decisions or in doctrinal works. Therefore, from our point of view, it seems that the test is reasonable.

Martin Maisner brought an interesting notion in his article concerning automatic processing of data during providing a service.[9] He writes: "*It is not possible to*

[7] The company was known for its aggressive advertisement practices, which were on the limits of legally permissible.

[8] Decision of the City Court in Prague from 12 January 2015, No. 66 C 143/2013. It was confirmed by the decision of the High Court in Prague from 13 October 2015, No. 3 CO 36/2015.

[9] See in Czech: Martin Maisner "Pasivní vs. aktivní hosting: hranice režimu Safe Harbour" [Passive vs. Active Hosting: Safe Harbour Boundaries], *Bulletin advokacie,* Česká advokátní komora, 2017.

take out of the context one of the conclusions of the L'Oréal v. eBay ruling that the provider plays an active role for specific content in a situation where he optimizes the presentation of the content, without taking account to the facts of that decision. In order for the provider to be judged as being active on the specific content, it must be clear from the provider's activity that the data stored in the activity is known to him or controlled by him. If eBay had registered the search engine optimization keywords, it had to know what words to register, which is the content on its site." Maisner continues that it would be problematic to apply the rules set by the decision in situation, when the optimisation is done automatically without actual knowledge of the content.

In our opinion, this issue will have to be solved in the future.

Question 1.1.3.
Existing Czech case law does not show that there are any major problems with the notice-and-take down regime. In our opinion, use of this system for the enforcement of absolute rights (e.g. intellectual property rights) is appropriate.

Question 1.1.4.
Unfortunately, we cannot provide an answer to this question. Decisions of first instance courts are generally not published (they are generally provided only upon a request). Therefore, it is very hard to tell any statistics.

A case concerning a privacy claim and injunction is elaborated in detail as a part of answer for question No. 4.4.

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.
Originally, the remedies concerning issues in the cases, where the consumer is one of the contracting parties, were implemented to the Czech law by the Act No. 40/1964 Sb., Civil Code, as amended. The main legislation was incorporated in the Section 619 et seq. stating that the guarantee period was before 2002 set for the 6 months. After 2002 it was harmonized in accordance with the Consumer Sales and Guarantees Directive and the period was set for the 24 months. This "old" Civil Code was however replaced by a "new" one (Act No. 89/2012 Sb., Civil Code, as amended) effective from 1 January 2014. The basis for deciding on the remedies for the consumers is incorporated in Section 2165 et seq. as the

Available online: http://www.bulletin-advokacie.cz/pasivni-vs.-aktivni-hosting-hranice-rezimu-safe-harbour?browser=full.

rights arising from defective performance.[10] As the "new" Civil Code is rather new, there is no relevant case law concerning the topic. It is, however, possible to use older case law as the provisions of the "old" Civil Code and "new" Civil Code are not that different (this is also supported by scholars).

It is necessary to mention that the legislation on such topic was rather clearly defined by the "old" Civil Code, thus there are generally not so many relevant cases (we are mentioning it further in the text). The situation is, however, different under the "new" Civil Code, as the formulation gives some space to the different types of the interpretation, especially of the guarantee period (6 to 24 months). In our opinion, such debate is not relevant and such period should last for 24 months as mention above (if there are no exceptions). It is thus generally assumed that case law will follow the same ideas as it did, when the "old" Civil Code was in effect.

The Supreme Court explicitly mentioned that a rebuttable presumption stating that the conflict with the purchase contract, which occurred within six months of taking over the goods by the buyer, existed already upon its takeover, also applies to the used goods.[11] This does not mean that the seller has the obligation to guarantee the quality of the used goods; however, the quality of such goods cannot be in contradiction with the contract. This was also confirmed by the Supreme Court, which stated that statutory guarantee does not apply to the used goods, even if the buyer is the first purchaser of such goods.[12] The seller can however offer the guarantee on the used goods when explicitly stated between the parties on the contractual basis (the contract itself, however, does not have to be in a written form).[13] It has to be generally stated that seller's liability (guarantee) covers all defects that occurred during the warranty period as a conflict with the purchase contract, regardless of whether they existed already at the time of the takeover of the goods and occurred subsequently or originated only after the moment the buyer took over the goods.[14] The seller cannot extend the rights of liability for defects (of new goods) to entities other than the buyer even by a declaration in the warranty card.[15]

[10] We do not see as adequate to copy relevant Sections to the text itself, thus we suggest seeing full translation of the new Civil Code. Such translation is not official, however it was provided by the Czech Bar Association. Available online: http://www.cak.cz/assets/pro-advokaty/mezinarodni-vztahy/civil-code.pdf

[11] The decision of the Supreme Court of the Czech Republic from 26 October 2010, No. 33 Cdo 2281/2008.

[12] The decision of the Supreme Court of the Czech Republic from 26 October 2010, No. 33 Cdo 2281/2008.

[13] The decision of the Supreme Court of the Czech Republic from 26 October 2010, No. 33 Cdo 2281/2008.

[14] The decision of the Supreme Court of the Czech Republic from 23 February 2016, No. 33 Cdo 3744/2015.

[15] The decision of the Supreme Court of the Czech Republic from 29 July 2004, No. 33 Odo 329/2004.

We have mentioned mainly older decisions dealing with specific sections of the "old" Civil Code. We did this because it is generally expected that such interpretation will be likely followed also when interpreting relevant Sections of the "new" Civil Code as the legislation is rather similar. The above mentioned case law deals only with some specific questions because the standards described in this section were partly in place even before the Consumer Sales and Guarantees Directive was implemented to the Czech law.

Question 1.2.2.

As it is stated by the European Commission and also by the directive itself (and as it is connected with the policy of digital single market), it is seemed as welcomed step to achieve such goal also by us, as it indicates higher consumer protection in the European Union. The harmonization of the legislation should lower the expenses of the entrepreneurs to manifest compliance with the legislation of the different Member States. We see the greatest benefit for consumers in a form of an access to more digital products, often at better price or better quality. At present, it may be problematic to enforce consumer rights related to the delivery of digital content because specific remedies connected to such issue are not available at EU level. We thus support full harmonization.

We support, in particular, new basic principles and institutions, on which the proposal is based, namely the right of consumers to terminate contracts concluded for a period longer than one year and the rules on the supplier's options for changing digital content. This should be for the benefit of the consumers.

We consider recital 17 of the directive to be misleading and we would recommend more appropriate argumentation, why it is mentioned here in such form. We do not see major difference in the provision of digital content in connection with any kind of device that is capable of communicating online. Devices falling under the category of Internet of Things are difficult to define and, in our opinion, should not be excluded from the Directive (possibly stating more specific reasons why this has happened or at least some explanation in the Explanatory Memorandum would help the situation).

We would also like to point out inaccurate translation of some of the provisions into the Czech language (e.g. Recital 32 or 44). There is also possible risk of inappropriate interpretation of the Article 10 (a). This article could be interpreted wider than it is desirable. It would be preferable to specify digital content – such content as it is provided to the consumer by the supplier on the basis of a reciprocal contractual arrangement.

Question 1.2.3.

We support full harmonization of the legislation also in this respect and we are following similar argumentation as in the previous question to support that.

We agree with the fact that it is inappropriate to apply other rules for liability for defects in distance-selling goods (including online selling) and for goods sold in classic shops. This is also stressed out in the draft document itself, pointing to the situation, where the entrepreneur provides both sales opportunities. However, it is not appropriate to further state in the proposal that such businesses will not be exposed to additional costs or that any costs will not be significant. According to our information, the Czech Republic also prefers that the approved rules on certain aspects of the sale of goods and guarantees should apply irrespective of the form of the sale.

We agree that the consumer may terminate the contract even in case of minor defects (this was not allowed under the Consumer Sales and Guarantees Directive). We further agree with the deletion of the possibility for Member States to impose on consumers the obligation to inform the seller of a breach of the purchase agreement within certain period.

With regards to one of the most significant changes, which is the extension of the six-month to two-year period of the reversed burden of proof, a number of objections can be expected (in particular from the Member States where the level of consumer protection will be reduced in some respects). However, the extension of this period is, in general, a very important step towards increasing the level of consumer protection (which could serve as an argument for the above-mentioned Member States as well). It can also be stated that the unification of such period (the length of time for the exercise of rights of liability for defects and the reversed burden of proof) will strengthen the legal certainty of participating parties.

However, we see the requirement of the obligation of the entrepreneur to collect the goods from the consumer in the event of an exchange due to inconsistency with the remaining refund options (Article 10 (1)) as a relatively problematic and costly one. It is also potentially problematic to require the consumer to pay for the reduced value of the goods when terminating the contract (Article 13 (3) (d)). We find as unsuitable to have the possibility to shorten the time limit for the use of one-year liability for used goods (as regulated by the Consumer Sales and Guarantees Directive). We also noticed some faulty translations to the Czech language (e.g. Recital 16, 17, 19) and few grammatical mistakes (e.g. Recital 19).

Question 1.2.4.

Some of the arguments have already been outlined above. We generally welcome efforts to harmonize periods and specific procedures within the Member States, and we find this to be a positive step related to the completion of the Digital Single Market strategy. In general, we are, however, still worried (for example by a lower level of harmonization following any further adjustments to the legislation

in question) of the fragmentation of the specific provisions at Member States' level (although we are aware of the full-harmonization approach mentioned also in the footnote to this question).

We are also concerned that the relatively confusing situation around consumer protection would suffer even more. As a negative example we can mention consumer ADR / ODR dispute resolution in EU. Although the legal regulation had the potential to provide effective out-of-court dispute resolution (as it was proven by private sector), it did not meet the positive response in some Member States; the legal regime also created complicated scheme and another (parallel) mechanism for resolving consumer disputes.[16] This means that the consumers are orienting themselves in the field even less (which was really not the target of the legislation) – we are then generally pointing out the rigidity of the legal norms and the hypertrophy of legislation. In general, we, however, welcome the idea of harmonization at this level and we believe that it will ensure a higher level of legal certainty for all stakeholders.

Question 1.2.5.

The first possible problem we see in this specific question is fragmentation of the legal regime while interpreting, the term intermediary (online platform). Some states or providers (e.g. in Italy) are (in the cases of travel services) using the interpretation under the International Convention on Travel Contracts.

Also, on the basis of E-Commerce Directive, the online platforms are traditionally excluded from the liability connected with the contract between the consumer and the provider of the service itself (e.g. accommodation) and the terms and conditions set by the intermediary (containing the clauses excluding their liability) are generally considered as compatible with EU consumer protection law. Even as the consumer protection is regulated under the mentioned Directives, there is still general uncertainty of the consumer whether to use specific online platform or not. This can be seen in different approaches of the Member States in the question of Uber B. V., the online platform providing connection between the driver and the consumer. In this particular case, the main issues are, however, connected not to the consumer protection itself, but mainly to taxation, unfair competition or necessity of specific permissions (as for taxi

[16] For more on problematic questions connected to such legal regime see: Pavel Loutocký "Online Dispute Resolution to Resolve Consumer Disputes from the perspective of European Union Law: Is the Potential of ODR Fully Used?", *Masaryk University Journal of Law and Technology*, Masaryk University, 2016, vol. 10, issue. 1, p. 113-127, or Pavel Loutocký "Mimosoudní řešení spotřebitelských sporů online v právu EU" [Alternative consumer disputes resolution online under the EU law]. Advanced Master's Thesis. In Czech available online: https://is.muni.cz/auth/th/210290/pravf_r/?lang=en

drivers). It, however, still can confuse the client whether such platform is offering its services in accordance with the law.

We would be very careful in such situation to regulate online platforms on the basis of consumer protection more precisely. Both the market and the online platforms are constantly developing, also thanks to the opportunities offered by the current relatively open legal framework. Restricting the functions of the online platforms can lead to slowing down of innovations in this area and even to the disruption of the very nature of their operation. Excessive and unbalanced regulation of online platforms could therefore have adverse consequences for the provider, the user or the market itself. The above mentioned legal background offers in our opinion a decent framework so far. Even though there are more opinions on regulating the area,[17] we are worried that a more rigid legislation would complicate the situation even further and in the end, it could also further confuse the consumer (as it is happening in other areas of consumer protection law mentioned above).

Question 1.2.6.

We are not aware of any relevant Czech case law on that issue. The case law connected with online platforms is mainly focused on the other issues than consumer protection. In Czech Republic, as in other Member States, many core questions with regard to online platforms remain unclear, e.g. the legal position of Uber.

Question 1.2.7.

We suppose that the formulation of this question is not "*to expand the scope of the rules on Business to Consumers (B2C) to Business to Consumers (B2B)*" but "*to expand the scope of the rules on Business to Consumers (B2C) to Business to* ***Business*** *(B2B).*" If that is correct, we do not share the opinion that such expansion would be necessary. Some scholars are pointing out that even in B2B relations one party could be disadvantaged,[18] but, also in coherence with abovementioned, we do not see such regulation as beneficial, as it would complicate the problematic area of legal regulation of online platforms even more.

[17] Such as Margherita Colangelo, Vincenzo Zeno-Zencovich "Online Platforms, Competition Rules and Consumer Protection in Travel Industry", *Journal of European Consumer and Market Law.* Available online: https://ssrn.com/abstract=2758347

[18] In the Czech Republic e.g. Josef Bejček "Smluvní svoboda a ochrana slabšího obchodníka" [Contractual freedom and protection of a weaker entrepreneur]. 1. ed. Brno: Masaryk University, 2016. 516 p. Editio Scientia, vol. 57.

1.3. Geo-blocking

Question 1.3.1.
We suppose that the formulation of this question is not "*... the interlink between this Regulation and Regulation 1215/2015 on the issue ...*" but "*... the interlink between this Regulation and* ***Regulation 1215/2012*** *on the issue ...*" If that is correct, we understand the question as aiming on the mechanics behind the Article 1 subsection 5 of the proposed Regulation in the interaction with the Section 4 Jurisdiction over consumer contracts of the Regulation 1215/2012.

We are in full support of the harmonization efforts that further the free movement of digital goods and services within the Single Market such as the proposed Regulation. At the same time, we see the consumer protection as a significant tool for achieving the overcoming of embedded differences between the national markets of the Member States.

The proposed Regulation could in our opinion lead to increased diversity of cross-border consumer-trader relationships, which would require more frequent assessment under the Regulation 1215/2012 regime for determining of jurisdiction. This may present additional burden on certain traders, as these jurisdiction rules serve the purpose of relatively strengthening the consumer's position in case of legal dispute. It is, however, in our view necessary to accept this as part of the cost for addressing the issue of unjustified geo-blocking and increasing the coherence of the European digital single market.

1.4. Questions related to the collaborative economy

Question 1.4.1.
One of the main issues, which was already referred to in this report, is connected with using the transportation platform Uber. As in other Member States, the problematic questions are rather similar and mainly connected with the necessity to obtain special type of licence (see more on that in the question 1.4.3 and partly 1.4.2) or with competition issues (see more on that in the question 1.4.2). This does not, however, mean that the issues raised by collaborative economy business are connected only to transportation. In the moment, the municipality of the capital city of Prague is thinking about regulating accommodation services arranged through the Airbnb platform, as accommodation services of this type are almost not regulated. The presented idea is to better enforce the compliance with the obligations, especially by the property owners. The inspiration seems to be partly taken from e.g. Amsterdam, where it is allowed to rent an apartment for up to 60 days a year. These ideas are, however, still not in any way supported by any legislative activity (or by local regulation). There is further also the matter of Czech provider of peer-to-peer lending. The platform is called

Zonky.[19] The main principle is based on the wide community, which crowdfunds the loan to the interested person for lower rates than available through traditional lending. The main issue is connected with a lack of liability in the case the money is not repaid. The principle is the same as in the above mentioned case of accommodation and the platform itself has limited liability.

Question 1.4.2.

The issues connected with collaborative economy in the Czech Republic are nowadays mainly connected with transportation provider Uber. We will thus focus further on this provider. This will however hopefully serve as general indication of the main concerns connected with collaborative economy in the Czech Republic.

The issue in this question has to be divided into two situations. The first one is connected with unlawful distortions of competition regulated by the Act No. 143/2001 Sb., Act on Protection of Competition and on the Amendment of Certain Acts (Act on Protection of Competition), as amended, thus falling under public law regulation. The second one is connected with unfair competition defined by the Section 2972 et seq. of the Civil Code, thus falling under private law regulation.

We are generally of the opinion that collaborative economy should not be regulated in the moment by public law regulation of unfair competition, as the Act on Protection of Competition states in the Section 19a that the public authorities should not generally intervene in competition, if specific services are procompetitive (and we argue that Uber is procompetitive). It is, however, question for further discussions, if some of the providers are not infringing upon the Article 101 para. 3 of TFEU, or similarly upon Section 3 of the Act on Protection of Competition.[20]

It is shown by the practice of the most of the European countries, that the major "fight" against collaborative economy (and especially Uber) is raised under the issues of the unfair competition in the meaning of private law (or pertinently in connection with specific permission).[21] The lawsuit is usually filed by an association representing taxi drivers arguing that Uber is violating standards on the market, that it is against unfair competition rules, or that it is against good manners of competition. This situation falls under general clause defining unfair competition.[22] Everyone, whose law has been infringed (competitors,

[19] Zonky. Available online: https://zonky.cz/

[20] We can also raise the question, if such procedure would be effective and the practice shows that private law mechanisms (with using an interim measure) are preferred.

[21] This has happened e.g. in Belgium, Italy, Germany or Spain.

[22] Section 2990 of the Civil Code also states that *"A person whose right has been jeopardised or violated by an unallowed restriction of competition has the rights provided under Section 2988."*

consumers or legal person defending the interests of such subjects) can claim protection against unfair competition under the rules of the Civil Code. To fulfil general clause, it is then necessary to fulfil three conditions cumulatively: (i) business conduct, (ii) a conflict with good manners of competition and (iii) the ability to cause harm to other competitors or customers. The first condition (business conduct) is in this case clearly fulfilled. The third condition (harm to the other competitors) is in those cases fulfilled as well and it is seen in real migration of the customers to the drivers using Uber from the taxi drivers. The second condition (good manners of competition) causes the most problems. The issue was also partly analysed by the Advocate General in the case of Asociación Profesional Elite Taxi v Uber Systems Spain SL.[23] It was, however, said here that final decision should be kept on the national legislation. There are two different opinions in the Czech Republic. One is generally saying that Uber is circumventing Czech law, especially the Act No. 111/1994 Sb., Road Transportation Act, as amended, thus being unfair competition[24], the second one (which we are supporting) is generally saying that the regulation of taxi services incorporated in the Road Transportation Act is not covering the issue of Uber (thus it does not violate the rules of unfair competition). Such opinion was also supported by the Municipal Court in Prague[25], which said that the driver using Uber application cannot be seen as the person illegally working as a taxi driver.[26] This does not, however, mean that Uber would not be sued by taxi services under private law. Such law suits are pending at the moment and we are unaware of any final court decision. The Regional Court in Brno (second biggest city in the Czech Republic), however, banned by its interim measure the use of Uber, as it is against the law and local regulations. Between the other arguments, it was said that the drivers are not approved on the basis of the Road Transportation Act and thus Uber (which was the sued party in this case) cannot provide the services using unapproved drivers. Such decision was, however, overturned by the High Court in Olomouc (also reflecting the argumentation of Municipal Court in Prague as it was introduced above). We are thus waiting for another decision of the Regional Court in Brno as the situation still remains unclear. We are, however, of the opinion that Uber as the provider cannot be banned in whole because it would be against euro-conform interpretation and also not in coherence with E-Commerce

[23] Opinion of Advocate General of the CJEU Maciej Szupnar in the case of C-435/15, Asociación Profesional Elite Taxi v Uber Systems Spain SL from 17 May 2017.

[24] Jan Kupčík "Aplikace Uber z pohledu (nejen) soutěžního práva" [Uber application from the point of view of (not only) competition law], *Právní rozhledy*, C.H. Beck, 2016, issue 13-14, p. 496-501.

[25] We are not stating the exact date and number of the decision as it is not accessible from the information systems and the public was informed of the facts through the media.

[26] The court was, however, dealing here with the driver, not the Uber platform.

Directive. It could be, however, said that Uber has to change the rules applied to drivers (see more on that in the next question).

Question 1.4.3.

For the time being, the Czech Republic has not legislatively regulated individual providers of services related to the shared economy. In any case, the Czech Republic is strongly aware of the cross-border character of the collaborative economy, however, waiting for the clarification from the European Commission. We are also waiting for the results of the cases decided in the moment by CJEU to ensure that national rules are in line with the demands of the EU law. Uber itself does not fall under the definition of taxi services provider under the Road Transportation Act because it does not provide any transportation service. In our opinion it can be classified as taxi service dispatching department and there are no legal obligations put on such subject also on the basis of commentaries to the Road Transportation Act.

In the case of a specific activity of the subject offering the service via the platform, the situation is more complicated and, in connection with the abovementioned, public regulations should be kept in mind. The users offering service through platform thus have to fulfil the conditions required by the public law.

In the case of transportation, the question, whether the driver falls under the regulation of taxi driver or not, still remains unclear (as it was presented in the previous question). We are, however, of the opinion that such drivers do not fall under the scope of the Road Transportation Act. By the rigid interpretation of this Act one can say, that such drivers fulfil the definition of taxi. The definition is fulfilled (and the drivers are falling under the definition of taxi drivers), when they are not employed by taxi service provider itself and their object is transportation of persons. In our opinion, such an approach does not sufficiently reflect the broader context of the relevant legislation. We agree with the opinion of Kindl and Koudelka[27] that taxi service legislation in accordance with the Road Transport Act can only be applied to professional national providers of passenger transport for other peoples' need using vehicles with a capacity of up to 9 persons including the driver. However, drivers who share their personal vehicles using Uber are not seemed by us as those professional providers (this point of view is somehow similar with the general opinion of the Commission on that question). In any case, we still have to wait for the decision of the Czech courts. If the interpretation would be that Uber drivers fall under the definition of taxi drivers, then they will have to fulfil the conditions of Road Transportation Act,

[27] Jiří Kindl, Martin Koudelka "Regulatorní výzvy sdílené přepravy" [Regulatory challenges of shared transport], *Právní rozhledy*, C. H. Beck, 2017, issue 7, p. 229.

which are at least to establish business authorization (listed in trade register), current listing of taxi vehicles, recordings on transported persons (or more precisely all contracts on that) and taxi drivers licence. These demands would be, however, liquidating for the business itself.

The regulation of accommodation services is aimed mainly at the hygienic and safety regulations and the tax and notification duty of the accommodated guests. The hygienic regulations are governed by the Act No. 258/2000 Sb., On the Protection of Public Health. The service provider in accommodation establishments must introduce an operating code (the exception is, however, for accommodation in multi-dwelling buildings, family houses and individual recreation buildings) listing e.g. hygiene measures, measures on food and beverages, cleaning the house or sanitation and responsibility of individual workers. Such code is then submitted for the approval to the local public health authority.

The other services such as car sharing or crowdfunding are usually not specifically regulated (however, the public legislation e.g. on technical norms still has to be followed) and, as it was mentioned above, the Czech Republic is mainly waiting for the opinion of the Commission.

Question 1.4.4.

There are no issues connected with collaborative economy in the consumer disputes so far. This is also caused in our opinion by the fact, that the position of the consumer and the provider of the goods or service itself (not the platform) is somehow getting equal (which is the basic idea of peer-to-peer economy model). This does not, however, mean that those services do not have to be in compliance with consumer protection legislation and consumer protection is also accented in particular law regulation. E.g. in the Road Transportation Act it is explicitly mentioned more times that the consumer protection has to be fully respected while providing relevant services.

Question 1.4.5.

General definition of the trader is incorporated in the Section 420 and 421 of the Civil Code. The Civil Code is, however, using the expression "entrepreneur". Section 420 is stating that "*(1) A person who, on his own account and responsibility, independently carries out a gainful activity in the form of a trade or in a similar manner with the intention to do so consistently for profit is considered, with regard to this activity, to be an entrepreneur. (2) For the purposes of consumer protection and for the purposes of Section 1963, any person who enters into contracts related to his own commercial, production or similar activities, or within his trade, business or profession, or a person acting in the name or on the account of an entrepreneur is considered to be an entrepreneur.*" Section 421 is stating that "*(1) A person registered in the commercial register is considered to be*

an entrepreneur. The conditions under which persons are subject to registration in the commercial register are provided by another statute. (2) A person who is authorised to conduct his business activities on the basis of a trade or another licence under another statute is presumed to be an entrepreneur."[28] There is also specific definition of entrepreneur in the Act No. 634/1992 Sb., on the Consumer Protection. That is, however, similar to the presented definition.[29] There is no special provision which would focus on trader as one of the parties participating in collaborative economy.

Question 1.4.6.

One of the important conditions for legislation while dealing with new fenomenon is to be sufficiently open for new ideas and possibilities. This applies in our opinion also in collaborative economy. Thus we are against overregulation (and rigid regulation) of this field (as we already mentioned above). We think that rating systems in this field and also generally for consumer protection are one of the most efficient and needed instruments. We have also mentioned such view in our previous papers concerning EU consumer ODR regime.[30]

In our opinion evaluation mechanisms are crucial factors to determine the quality, reliability or oppositely the malfunction of the system (peer-to-peer platform) or unsuitable behaviour of the individuals, especially in the online environment. Such polarized information contributes to the further organization of the information society in a virtual environment and helps with its functioning. In this context, it is appropriate to use indirect self-regulatory mechanisms, which motivate the parties to act in a desired and expected manner. The publication of the feedback on the quality of services provided in conjunction with other rating mechanisms should thus be an important part to ensure proper effectiveness of such regime. Ecommerce Europe Trustmark could serve as an example of trustmark.[31] We thus suggest to use trustmarks to mark the platforms and reputation system to rate the users (including black lists or name and shame mechanisms). We think that such mechanisms should be sufficient to regulate the environment

[28] Unofficial translation.

[29] Moreover, it defines seller, producer, importer or distributor. All of those are, however, classified as entrepreneurs.

[30] Pavel Loutocký "Online Dispute Resolution to Resolve Consumer Disputes from the perspective of European Union Law: Is the Potential of ODR Fully Used?", *Masaryk University Journal of Law and Technology*, Masaryk University, 2016, vol. 10, issue. 1, p. 113-127, or Pavel Loutocký "Mimosoudní řešení spotřebitelských sporů online v právu EU" [Alternative consumer disputes resolution online under the EU law]. Advanced Master's Thesis. In Czech available online: https://is.muni.cz/auth/th/210290/pravf_r/?lang=en

[31] At the moment, we, however, have to keep in mind that the success of the trustmarks in general is not that evident as it was previously assumed, due to their large number, fragmentation and even possible lack of transparency.

privately without the intereference of state power, which already has proved many times as the most efficient solution (i.e. self-regulation).

2. Digital media

Question 2.1.

The framework of the EU Audio-visual Media Services Directive was implemented into the Czech legal system through the Act No. 132/2010 Sb. on On-Request Audio-visual Media Services and Amendment of Selected Acts, as amended. The several amendments of this act since its introduction concerned merely minor aspects related to introduction of other legislation, it thereby underwent no significant legislative changes since then. The academic and professional attention towards the discussion and interpretation of this area of law is to our knowledge limited to several articles and two commentaries dating back to the time of the introduction of this new legislation.

The authors of the commentary from 2012 originally inferred that the factor of the length of the program cannot be disregarded and shorter sequences may not be possible to be considered as programmes.[32] We however found no other instances, where this opinion would be shared or further developed by academics or the regulatory body. The CJEU judgement in case C-347/14 was therefore to our knowledge not reflected in any significant way in Czech national practice, as the concerned matter of the scope of interpretation of the term 'programme' was as far as could have been traced contested neither in front of the Czech regulator, nor the Czech courts.

With regard to the relatively small size of Czech audio-visual media market, there is only limited amount of activity on the side of the local regulator, the Council for Radio and Television Broadcasting (further referred to merely as "the Council").[33] The Council got timely acquainted with the CJEU judgement in case C-347/14,[34] there are, however, no indications that this judgement affected the activities of the regulator. The available documentation of its practice that we have at our disposal indicates no sign of deviation in the interpretation of the concept of 'programme' from the interpretation concluded by the CJEU.

[32] Vladan Rámiš, Mária Čuhelová, Alexandra Wünschová Pujmanová, Kateřina Hrubešová "Zákon o audiovizuálních mediálních službách na vyžádání. Komentář." [Act on On-Request Audio-visual Media Services. Commentary.] Linde: Praha, 2012, p. 24.

[33] Further information about the Council may be found on its website. Available online: http://www.rrtv.cz/en/

[34] *Tisková zpráva z 21. zasedání, konaného dne 18. 11. 2015* [News report from the 21st session, which took place on 18 November 2015]. In Czech available online: http://www.rrtv.cz/cz/files/press/TZ_21_15.pdf

Question 2.2.
The continuous transformation of the audio-visual media landscape requires occasional adaptation to the new developments. The increasing penetration of the society through the content originating on video platforms necessitates in our view an extension of the AVMS rules in this direction.

The dissemination of hate speech is currently a strongly publicized topic not only in Czech Republic, but worldwide, instigated in some regards through the opinions and statements by the political representation. Popular concerns for curbing this rise of hate speech and disinformation lead to questionable legislative actions, e.g. the highly discussed German *Netzwerkdurchsetzungsgesetz*. We perceive the extension of rules on protection of minors and the combatting of hate speech to the video platforms under the proposed amendment of the AVMS directive in this relative perspective as a sensible legislative proposal, which presents an adequate measure for reaching the intended goal without unreasonably burdening any of the affected parties.

In our opinion it is necessary to seek an adequate balance between the level of regulatory intervention on one hand and the extent of threat to the values protected by this regulation. Given the nature of the original content uploaded to the video platforms, specifically various personal, video game, life or other vlogs, there is certainly a potentially broad grey area of conflict between the need for regulation of this new form of semi-commercial communication and threat of principal intervention into the freedom of self-expression and self-presentation of the individuals. From our personal perspective the current state of vlogging does not justify an extension of the scope of application for the rules on commercial communications.

We are not aware of sector-specific rules for audio-visual platforms in the Czech legal environment.

Question 2.3.
We are not aware of such a decision by the regulator with regard to the audio-visual media services. As already mentioned in Q2.1, the Czech audio-visual media market it relatively small and enjoys only limited attention from the Council for Radio and Television Broadcasting in comparison to services that fall under the radio and television broadcasting regulation.

Question 2.4.
The Czech regulator, the Council for Radio and Television Broadcasting, is formally established as a central administrative body, it does, however, stand apart from the traditional administrative hierarchy and it does retain in effect an

independence from the executive branch of the government.[35] The members of the Council are formally named and dismissed by the prime minister, his action must, however, be based on a nomination from the Chamber of Deputies.[36] One of the grounds for dismissal is an action of a council member, which would call into question the impartiality or independence of the council member or impartiality of the council.[37] The functional independence then follows from so called "free mandate"[38] and the incompatibility with political functions.[39] Another important aspect indicating the independent position of the regulator is impartiality, expertise and objectivity of the office.[40] The Council also retains sufficient level of budgetary independence, as it operates with a separate budget covered by independent chapter of the Czech Republic State budget.[41] The status of the media regulator in the Czech Republic is thereby largely similar to the status of the telecommunications or data protection regulators.

With regard to the national organisation of the regulatory body, an EU level introduction of independence requirement would merely reinforce the status of the Council. We are, however, of the opinion that the organisational nature of the administrative bodies should primarily be structured through the national legislation.

With regard to the goal of facilitating the creation of European single market for the audio-visual media services, we do not perceive the aspect of independence of the national regulator as the principal obstacle to its creation. In our view the primary cause for the fragmentation of this market is connected with the territorial nature of intellectual property licencing, as well as cultural and linguistic diversity of the Member States, which creates natural barriers to unification of audio-visual media services.

[35] Jan Drdla "Rada pro rozhlasové a televizní vysílání a její partneři ze Středoevropského fóra regulátorů" [The Council for Radio and Television Broadcasting and its partners from the Central European Regulatory Forum] Academic thesis. Masaryk university: Brno, 2012/2013. In Czech available online: https://is.muni.cz/th/210296/pravf_r/RIGOR.pdf . p. 45.

[36] Section 7 subsection 5 of the Act No. 231/2001 Sb. on operation of radio and television broadcasting.

[37] Section 7 subsection 7 letter c) of the Act No. 231/2001 Sb.

[38] Requirement of personal performance of the function and prohibition of any form of directions or instructions. Section 7 subsection 10 of the Act No. 231/2001 Sb.

[39] Section 7 subsection 9 of the Act No. 231/2001 Sb.

[40] Jan Drdla "Rada pro rozhlasové a televizní vysílání a její partneři ze Středoevropského fóra regulátorů" [The Council for Radio and Television Broadcasting and its partners from the Central European Regulatory Forum] Academic thesis. Masaryk university: Brno, 2012/2013. In Czech available online: https://is.muni.cz/th/210296/pravf_r/RIGOR.pdf . p. 52.

[41] *Ibid*. p. 54.

Question 2.5.

The identification of the most contentious issues necessitates an assessment of the sector from a subjective perspective, which may greatly differ depending upon the position of the observer. Given that we cannot provide accurate representation of the perspective held by the media service providers and that our perspective as spectators is too narrow to encompass the breadth of the sector, we refer in this part largely to the position officially presented by the Council.

If we attempt to take the perspective of the regulator, the 2016 Annual Report[42] indicated several areas of priority interest. In the last year, the Council focused on the issue of children protection from negative effects of broadcasting with focus on the content of the crime programs.[43] It observed positive development and significant decrease of unsuitable content for minors in all forms of broadcasting in comparison to the previous analysis it undertook five years ago. Another priority was related to the last year's regional and senate election and aimed for balanced and objective pre-election broadcasting.[44] As there are important parliamentary and presidential elections to be held this autumn and next spring respectively, the importance of this issue remains high. Further priorities deal with traditional issues like media literacy, consumer protection in commercial communication or cybersecurity.[45] The Council was also actively participating in the revision process of the AVMS Directive, above all through its membership in ERGA.[46] The priorities mentioned above remain largely relevant for the year 2017 with and additional focus on the analysis of the HbbTV (Hybrid Broadcast Broadband Television) technology.[47]

A specific issue that gradually gained with respect to the relatively marginal real impact on the Czech Republic largely disproportionate media coverage is the migration crisis. Stimulated through populistic political statements the media dedicated a lot of attention to all possible aspects of the migration issue. The Council undertook a large scale analysis in 2015, which showed several inclinations towards potentially unbalanced reporting.[48] The rise of xenophobic ele-

[42] Rada pro rozhlasové a televizní vysílání [the Council Radio and Television Broadcasting]. Zpráva o činnosti Rady pro rozhlasové a televizní vysílání a o stavu oblasti rozhlasového a televizního vysílání a v oblasti poskytování audiovizuálních mediálních služeb na vyžádání za rok 2016 [Report on the Activities of the Council for Radio and Television Broadcasting and on the Situation in the Sector of Radio and Television Broadcasting and in the Sector of On-Request Audio-visual Media Services for the Year 2016]. In Czech available online: http://www.rrtv.cz/cz/files/zpravy/VZ2016.pdf

[43] Ibid. p. 14.

[44] Ibid. p. 15.

[45] Ibid. p. 15-18.

[46] Ibid. p. 18 and 37.

[47] Ibid. p. 18-20 and 26.

[48] Ibid. p. 20-21.

ments in the local public sphere presents at this point in our opinion the most serious issue for the media sector, particularly for the media that communicate their content through alternative channels, e.g. audio-visual media services. Given the lack of strict rules for content comparable with the broadcasting regulation, the audio-visual media may pose as one of the sources for anti-migration and xenophobic discourse, eventually extending to a level of hate speech. The prevention against dissemination of this kind of content constitutes in our opinion one of the areas, that could be further developed.

Question 2.6.

The major initiative for targeted advertising on television currently underway is the introduction of HbbTV features by several major commercial TV stations. The first pilot projects started about two years ago. Currently, HbbTV targeted advertising is solidifying its presence on the Czech screens. The forms it takes at this point are the blue or red dot for suggested content, switch-in advertisement, or frequency capping. The targeting is gradually moving beyond mere program or regional targeting and in Q4 2017 are expected first cases of behavioural targeting.[49] The legality of this behaviour is yet to be contested in front of the regulators. The data protection authority did not yet concern itself with any case dealing with HbbTV, which may change with the introduction of the behavioural targeting later this year.

The Council for Radio and Television Broadcasting recognized this trend in the 2016 Annual report and set for itself a priority for 2017 to analyse and reflect upon the potential need for regulatory re-adjustment in the light of this technological development.[50]

With regard to the current advertisement regulation, TV broadcasting regulation and data protection regulation in place, we do not find an urgent need for specific EU-wide harmonized approach. Despite the potential deep intrusion into the private sphere of the viewers, the HbbTV technology does not seem to create a new dimension that would fall entirely outside of the scope of the currently established regulative framework. Additionally, the early stage of its

[49] Co přináší spojení HbbTV reklamy a programatiku [What does the connection of HbbTV advertisment and programmatic purchase bring] *Mediaguru*. 22.6.2017. In Czech available online: https://www.mediaguru.cz/2017/06/co-prinasi-spojeni-hbbtv-reklamy-a-programatiku/

[50] Rada pro rozhlasové a televizní vysílání [the Council Radio and Television Broadcasting]. *Zpráva o činnosti Rady pro rozhlasové a televizní vysílání a o stavu oblasti rozhlasového a televizního vysílání a v oblasti poskytování audiovizuálních mediálních služeb na vyžádání za rok 2016* [Report on the Activities of the Council for Radio and Television Broadcasting and on the Situation in the Sector of Radio and Television Broadcasting and in the Sector of On-Request Audio-visual Media Services for the Year 2016]. In Czech available online: http://www.rrtv.cz/cz/files/zpravy/VZ2016.pdf. p. 8.

development and limited experience with its direction do not provide in our view a sufficient ground for appropriate assessment of the specific issues that could emerge as a consequence of this transition in the television advertisement strategy. An introduction of regulation focused on this specific issue would therefore be in our view preliminary.

Question 2.7.

The Czech copyright regime did not operate with specific regime for copyright licencing in case of satellite broadcasting as did some other EU Member States. After joining the EU in 2004, the Czech Act on Copyright[51] was merely amended in the harmonization procedures to include the legal definition of the term "satellite" pursuant to Article 1 subsection 1 of the Directive 93/83/EEC. The copyright licensing for TV and radio broadcasting is thereby subject to standard licensing procedures, commonly taking place through the collective licensing. [52]

We are not aware of any specific copyright licensing regime being applied under the Czech law to online transmissions of broadcasting organisations.

Question 2.8.

The barriers to cross-border portability of digital content are connected to the territorial nature of the intellectual property licencing regime. To our knowledge this was the main topic of the prolonged discussion in the European Union that led to the adoption of the Regulation 2017/1128 on cross-border portability of online content services in the internal market on the 14 June 2017.[53] As this regulation comes into force on 20 March 2018, the current intermezzo may still suffer from the identified issues related to aggravated cross-border portability of digital content; however, the new regulatory regime is aimed at overcoming these issues.

The access to information about the country of residence represents necessary information for pursuit of legal obligations in form of conformity with the territorial limitation of the rights to intellectual property. The principle of data minimisation under the GDPR should be in our opinion applied from the relative perspective of the personal data processed in the pursuit of the lawful purpose of the processing. In the context of the personal data processing for the

[51] Act No. 121/2000 Sb., on Copyright and Rights Related to Copyright and on Amendment to Certain Acts (the Copyright Act), as amended.

[52] Ivo Telec, Pavel Tůma *Autorský zákon: Komentář.* [The Copyright Act: Commentary] Praha: C.H. Beck, 2007. p. 253-254.

[53] Regulation 2017/1128 of 17 June 2017 on cross-border portability of online content services in the internal market. Eur-lex. Available online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32017R1128

purpose of compliance with the intellectual property regime, the data minimisation principle does in our opinion dictate the limitation of the personal data processed to the most general territorial unit relevant for this assessment, i.e. the country of residence. Processing of more detailed localisation data, e.g. the address of residence, would represent a case of divergence from the data minimisation principle. Similar conclusion can be drawn from the Recital 28[54] and Article 8 of the Regulation 2017/1128.

3. Digital infrastructures

Question 3.1.

There was no hard law to regulate net neutrality as a part of the Czech legal order. However, the Czech telecommunication office (the Czech national regulatory authority, further referred to merely as "the Office") issued in January 2014 a soft law document called "*General rules and recommendations for use of data traffic management in providing an Internet access service*" (further referred to merely as "the Rules and Recommendations")[55]. This document was a result of task, which was assigned to the Czech telecommunication office in a national concept "Digital Czechia 2.0"[56]. After the Regulation 2015/2120 came into force, it replaced the Rules and Recommendations, which are therefore no longer in force.

In the introductory part of the Rules and Recommendations the Office states that up to date there were no complains or other signs of problems with degradation of electronic communications services. The Office also mentions *Questionnaire For The Public Consultation On The Open Internet And Net Neutrality In Europe*[57], which was answered for the EU Commission, and in which the Office already

[54] *"IP address checks performed under this Regulation should be conducted in accordance with Directives 95/46/EC (9) and 2002/58/EC (10) of the European Parliament and of the Council. In addition, for the purpose of verification of the subscriber's Member State of residence what matters is not the precise location of the subscriber, but rather the Member State in which the subscriber is accessing the service. Accordingly, data on the subscriber's precise location or any other personal data should neither be collected nor processed for that purpose. Where the provider has reasonable doubts concerning the subscriber's Member State of residence and carries out an IP address check to verify the Member State of residence, the sole purpose of such checks should be to establish whether the subscriber is accessing or using the online content service within or outside the Member State of residence. Therefore, in such cases, the data resulting from the checking of IP addresses should only be collected in binary format and in compliance with applicable data protection rules. The provider should not exceed that level of detail."*

[55] In Czech available online:
http://www.ctu.cz/cs/download/obecna_pravidla_a_doporuceni_pro_vyuzivani_rizeni_datoveho_provozu_19122013.pdf.

[56] In Czech available online:
https://www.mpo.cz/assets/cz/e-komunikace-a-posta/Internet/2013/4/Digi_esko_v.2.0.pdf.

[57] Answers are in Czech available online here: http://www.ctu.cz/cs/download/tiskove-zpravy/rok_2010/reakce-ctu-na-dotazy-do-verejne-konzultace-evropske-komise-o-neutralite-internetu.pdf

had mentioned several potential problems like differences between advertised and real connection speed and possible discrimination of some kinds of traffic in the process of prioritising data traffic management.

The rules of the Office are generally equivalent with the provisions of the Regulation. Rule No. 1 stipulates that several abilities must be ensured for the end users. It is:

- Ability to receive and send information /data according to the choice of the end user,
- Ability to use services and applications by end user choice,
- Ability to install own hardware and software, if it does not damage the network,
- Provision of contractually agreed quality of service in compliance with contractually agreed terms and providing transparent information about the services provided by the service provider.

Rule No. 2 sets that when providing Internet access service, discrimination, blocking or degradation of specific data flows is not allowed. Rule No. 3 sets exceptions from Rules 1 and 2. These exceptions are basically connected with fulfilling legal duties, or solving technical issues within the network.

Rule No. 4 sets a number of information, which must be provided to the end user in a clear, explicit and understandable way. It was e.g. information on quality of the service, possible derogations and possibility of exceptions according to the Rule No. 3.

Rule No. 5 offers a definition of "Internet access service" as the one, which follows rules 1, 2 and 3.

The Office included also thoughts of Fair Use Policy into the Rules and Recommendations – it stated in Rule No. 6 that the lowered speed must also be expressly stated in the contract.

Finally, Rule No. 7 explicitly states that service providers can offer services which do not follow rules 1, 2 and 3, but they must inform the users about the nature of the service (its limitations etc.) in a clear, explicit and understandable way.

The Rules and Recommendations of the Office did not contain an equivalent to the second part of Art 3 subsection 5 ("*Providers of electronic communications to the public, including providers of internet access services, may offer or facilitate such services only if the network capacity is sufficient to provide them in addition to any internet access services provided. Such services shall not be usable or offered as a replacement for internet access services, and shall not be to the detriment of the availability or general quality of internet access services for end-users.*").

Zero-rating is not forbidden by Czech law. As can be seen from the *Report of the Czech Telecommunication Office on the results of the implementation of Regulation (EU) 2015/2120*[58], zero-rating policy do exist in the Czech Republic, and is being monitored and evaluated by the Office.[59]

Question 3.2.

Unfortunately, we cannot answer this question, because the effects of Directive No. 2014/61/EC have not had chance to manifest themselves. Act No. 194/2017 Sb., on measures to reduce the cost of deploying high-speed electronic communications networks and on amendment of some acts came into force on 15 June 2017, more than 18 months after the date set in the Directive.

We are not aware of any special broadband measures.

Question 3.3.

Decision of the Supreme Administrative Court from 29 June 2011 No. 6 As 13/2011 – 175 was concerned with following issue: Company Vodafone Czech Republic requested an assignment of E – GSM spectrum range, because on 1 January 2008 there were freed 32 channels in the range 882 – 888/927 – 933 MHz. Vodafone Czech Republic claimed that these channels should be assigned to her for two reasons. Firstly, because she was the first to apply to it and secondly, because of preceding "historical inequality".[60] The Office denied the application of Vodafone Czech Republic because the company was not a holder of a licence needed for assignment of frequencies in E-GSM spectrum range at the time. Therefore, the freed channels were distributed between two other providers of electronic communications services, who were already holders of the licence. This decision of the Office was confirmed by the City Court in Prague (the first instance court). The Supreme Administrative Court dismissed the complaint and confirmed decisions of the Office and of the City Court in Prague. In its argumentation, the Supreme Administrative Court mentioned EU directive No. 2002/21/EC, which is implemented in the Act No. 127/2005 Sb., on electronic communications, as amended. Recitals of the directive stress out the necessity for creation of conditions for effective competition in the field of electronic communications in the time of transition from monopoly to competitive environment. Thus, the Court stated that it was necessary to obtain the licence in the transparent selection procedure and not on the basis of historical inequality.

[58] In English available online: https://www.ctu.eu/sites/default/files/obsah/stranky/159928/soubory/ctuberecnnimpquestionnaireen.pdf.

[59] Ibidem, p. 6.

[60] For a long time, there were two major providers of electronic communications, and Vodafone was not one of them.

We have not encountered any other court decisions concerning spectrum management.

Question 3.4.
Independence of the Czech telecommunication office is ensured by Section 109 of the Act No. 127/2005 Sb., on electronic communications, as amended. It reads as follows:

> *Section 109*
> *Elimination of the Conflict of Interests*
> *(1) Employees assigned to the Ministry [Ministry of Industry and Trade of the Czech Republic] or to the Office, the head of an organizational service working for the Minister of Industry and Trade, advisers and employees performing other activities (designated otherwise) for the Minister of Industry and Trade, and Deputy Ministers of Industry and Trade shall not pursue any business activities in the field of electronic communications, become members of any governing, managing or supervisory bodies of any undertakings engaged in business within the scope of this Act, carry out any advisory work or any other professional assistance in matters of electronic communications area, or otherwise act in favour of any such undertakings.*
> *(2) For the Council member, the obligation specified in Subsection 1 above shall remain in effect for 6 months after the end of his term of office. During that period, he shall continue receiving, on a monthly basis, a salary equal to the average monthly salary he had while he was in office.*
> *(3) The Council member may not be employed by the Ministry or perform any other gainful activity for the Ministry.*[61]

There were no questions raised concerning independence of the Czech telecommunication office or its executive officers.

4. Data in the digital economy

Question 4.1.
The Ministry of the Interior of the Czech Republic is the body, which is responsible for preparation of the bill, which will harmonise Czech legal order with GDPR, whereas the Office for Personal Data Protection functions only as a consultant. The new act is quite needed, since the current act No. 101/2000 Sb., on the Protection of Personal Data and on Amendment to Some Acts, as amended, includes several provisions, which collide with the new regulation – e. g. Section 5, subsection 2 letter d), which enables data processing, if the data were lawfully

[61] Unofficial translation published by the Ministry of Industry and Trade of the Czech Republic. Available online: https://www.mpo.cz/dokument75810.html.

published in accordance with special legislation, if it does not prejudice the right to the protection of private and personal life of the data subject.[62]

Such exceptions will not be enforceable, once GDPR is in force. However, the harmonising act is still urgently needed as it would be extremely difficult for a lay person to recognise, which provisions are in force and which are not. That would greatly increase legal uncertainty.

As is known to us, the Ministry has prepared a first draft of the bill, which was processed and commented internally within the departments of the ministry. This version was prepared as an amendment of the act No. 101/2000 Sb.[63] The ministry took a minimalistic approach. In very few sections, there were regulated several issues, like e.g. the journalist and media exemption. However, the review from the ministry departments must have been quite extensive because a new version of the bill was prepared. At the end of August, the Ministry released a new version of the bill for the external review conducted by other ministries and entitled bodies.[64] The first part of the bill harmonises GDPR, the second part implements Directive (EU) 2016/680, the third part regulates processing of personal data in the case of securing "defence and security of the Czech Republic", which means mostly the intelligence services purposes and other personal data processing excluded from the application of GDPR. This part is almost literally taken from the old act No. 101/2000 Sb., and thus it is quite absurd in several parts.[65] The fourth part of the bill regulates existence, structure and competences of the Office for Personal Data Protection and the fifth part regulates administrative offences. The bill should come into force on the same date as GDPR.

[62] English translation of Act No. 101/2000 Sb., on the Protection of Personal Data and on Amendment to Some Acts, as amended, is available online on the webpage of the Office for Personal Data Protection: https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1107&archiv=0&p1=1105

[63] We have received a text of the bill from the Ministry upon a request made under the Freedom of Access to Information Act. It was the version which was subsequently reviewed internally within the ministry.

[64] In Czech available online:
http://www.komora.cz/pro-podnikani/legislativa-a-normy/pripominkovani-legislativy/nove-materialy-k-pripominkam/128-17-navrh-zakona-o-zpracovani-osobnich-udaju-t-8-9-2017.aspx.

[65] E.G. Section 35 subsection 3 of the bill regulates legal grounds based on which the personal data can be processed (in the context of maintaining defence and security of the Czech Republic). It reads as follows: "*The controller may process personal data only with the consent of data subject. Without such consent, the controller may process the data:*
(a) if he is carrying out processing which is essential to comply with legal obligation of the controller;
(b) if the processing is essential for fulfilment of a contract to which the data subject is a contracting party or for negotiations on conclusion or alteration of a contract negotiated on the data subject's proposal;
(c) if it is essential for the protection of vitally important interests of the data subject. In this case, the consent of data subject must be obtained without undue delay. If the consent is not granted, the controller must terminate the processing and liquidate the data;
(d) if they were lawfully published in accordance with special legislation. However, this shall not prejudice the right to the protection of private and personal lives of the data subject, or

In our opinion, it is doubtful, whether the new act will be promulgated before the Regulation comes into force. Apart from standard legislative process, which can take several more months, we must consider the general elections, which are being held in November. This can cause even more prolongations. Even in case that the act is prepared on time, there will be a very short time between promulgation and enforceability. That is quite problematic, because recipients of the law do not have enough time to prepare for the change.

In the meantime, the Office for Personal Data Protection provides an information service on its webpage.[66] There are two introductory articles (*"GDPR in questions and answers"*[67] and *"10 mistakes about GDPR"*)[68] and there are also Czech translations of WP 29 Guidelines concerning GDPR published on the webpage of the Office.

Question 4.2.

There is a noticeable activity in numerous sectors with regard to the adaptation to the GDPR requirements, encouraged through increasing awareness by providers of legal and consultancy services. Given the undergoing process of change, we do not have an access to appropriate statistical data to assess the awareness about the new requirements in any other than broadly general way.

To our knowledge, the progress towards GDPR compliance differs with respect to various categories of regulated subjects. Large and international businesses are fully aware of the new requirements and allocate adequate resources to legal and organisational compliance.

We expect, on the other hand, that the approach of the small and medium businesses in the Czech Republic does not significantly differ from the situation in other EU Member States. In their case, based on our fractional perspective of the situation and various available data protection surveys among SMEs

(e) if it is essential for the protection of rights and legitimate interests of the controller, recipient or other person concerned. However, such personal data processing may not be in contradiction with the data subject's right to protection of his private and personal lives.
(f) if he provides personal data on a public figure, official or employee of public administration that reveals information on their public or administrative activity, their functional or working position, or
(g) if the processing relates exclusively to archival purposes pursuant to a special Act."

[66] In Czech available online:
https://www.uoou.cz/obecne%2Dnarizeni%2Deu%2Dgdpr/ds-3938/p1=3938.

[67] In Czech available online:
https://www.uoou.cz/obecne%2Dnarizeni%2Do%2Dochrane%2Dosobnich%2Dudaju%2Dv%2Dotazkach%2Da%2Dodpovedich/d-23790/p1=3938.

[68] In Czech available online:
https://www.uoou.cz/desatero%2Domylu%2Do%2Dobecnem%2Dnarizeni%2Dgdpr/d-23799/p1=3938.

from abroad,[69] we assume they possess only a limited awareness about the legal development in the area of data protection and make similarly limited efforts towards achieving timely compliance. The recent changes and developments in other crucial areas for doing business, particularly the gradual introduction of the electronic evidence of sales, focus the attention of the SMEs away from the matter of GDPR compliance.

Question 4.3.

We perceive the discussion about the issues related to these kinds of new technologies in the Czech Republic to be in its infancy. It remains so far primarily on the academic level of several scholarly contributions,[70] whereas the identified issues and controversial aspects majorly follow the suit of the discussions in countries with more advanced legal research in these areas. The legislative measures are at this point to our knowledge limited to action plans and exploratory memoranda summarizing the key aspects of given new technology from the perspective of the given governmental body. We are not aware of any judicial or regulatory decisions concerning specifically the legal issues originating from the nature of these new technologies. There are decisions, which include in the relevant context connection to the application of the new technologies, those do, however, not concern specific legal issues caused by their introduction, but merely reflect on their potential role in otherwise established legal issue.

The topic of Internet of Things is similarly to e.g. Germany primarily included in the broader discussion concerning the Industry 4.0. The trend towards digitalisation of the industry has a potential to have strong impact on the Czech economy and is therefore among others readily explored by Minister-

[69] E.g. Rebecca Klahr and others "Annex to Cyber Security Breaches Survey 2017", UK Department for Culture, Media & Sport. 2017. Available online: https://www.ipsos.com/sites/default/files/2017-04/sri-cybersecurity-breaches-survey-2017-annex.pdf; Verizon. *2016 Data Breach Investigations Report*. 2016. Available online: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf; Symantec. *Internet Security Threat Report 2016*. 2016. Available online: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[70] As an example, the following articles of Czech scholars deal with legal issues related to the new technologies: Tomáš Abelovský "Počítač ako sudca" [Computer as a Judge]. *Revue pro právo a technologie*. 2016, Vol. 7, No. 14; Eva Fialová "RFID and Consumers' Privacy Protection". *Masaryk University Journal of Law and Technology*. 2011, Vol. 5, No. 1.; Eva Fialová "Identity Management in RFID Application". *Masaryk University Journal of Law and Technology*. 2013, Vol. 6, No. 2.; František Kasl "Internet věcí a ochrana dat v evropském kontextu" [Internet of Things and Data Protection in the European Context]. *Revue pro právo a technologie*. 2016, Vol. 7, No. 13.; Alžběta Krausová "Legal Aspects of Brain-Computer Interfaces". *Masaryk University Journal of Law and Technology*. 2014, Vol. 8, No. 2; Petra Krupičková "Smart contract – revoluce v smluvním právu 21. století?" [Smart Contract – Revolution in Contractual Law of the 21st Century?] *Revue pro právo a technologie*. 2017, Vol. 8, No. 15.; Eva Žáčková "Man-computer Symbiosis as a Way of Human Cognitive Enhancement". *Masaryk University Journal of Law and Technology*. 2011, Vol. 5, No. 1.

stvo průmyslu a obchodu [Ministry of Industry and Trade] in the memorandum called *Iniciativa Průmysl 4.0* [Industry 4.0 Initiative].[71] The identified legal issues relate to complexity and fragmentation of the legal framework,[72] lacking interoperability standards[73] and personal data processing and cybersecurity risks.[74]

The regulation and implementation of automated cars is currently a topic for Ministerstvo dopravy [Ministry of Transport], which recently issued a draft memorandum *Vize rozvoje autonomní mobility* [Visions of development of autonomous mobility][75] with an outlay of possible steps towards introduction of automated cars to Czech traffic system. There are, among other aspects, discussed the crucial legal issues that need to be addressed, particularly the matter of liability in a case of harm. The current Czech legal framework is based on the approach of liability of the driver. There are currently no indications that this regime should change; it is, however, still in an early stage of the discussion. However, as noticed in the framework document for the freight transport, the introduction of the higher level of automated cars may cause decline in driving skills, due to lack of experience and increasing reliance on the automated features.[76] This aspect of the innovation will need to be reflected in the assessment of the driver's liability, particularly in case of non-professional drivers.

Further specific issues relate to the development of the smart infrastructure. This area contains a myriad of sector-specific regulatory and organisational requirements that need to be review in the light of increased connectivity, cyber-physical nature of the components and diverse technical standards. For some of the core areas an action plan on the governmental level is readily available and the main topics are identified. As an example we can point to the *Akční plán rozvoje inteligentních dopravních systémů (ITS) v ČR do roku 2020 (s výhledem do roku 2050)* [Action Plan for the Development of the Intelligent Transport Systems (ITS) in the Czech Republic until the Year 2020 (with an Outlook to the Year 2050)] by

[71] Ministerstvo průmyslu a obchodu [Ministry of Industry and Trade] *Iniciativa Průmysl 4.0* [Industry 4.0 Initiative] 2.9.2016. In Czech available online: https://www.mpo.cz/cz/prumysl/prumysl-4-0/iniciativa-prumysl-4-0--176055/

[72] *Ibid.* p. 108.

[73] *Ibid.* p. 114.

[74] *Ibid.* p. 115.

[75] The document is currently still in the inter-ministerial comment procedure and thereby not available to the public. Public was informed of its general contents through the media.

[76] Ministerstvo dopravy [Ministry of Transport]. *Koncepce nákladní dopravy pro období 2017-2023 s výhledem do roku 2030* [Concept of the Freight Transport for the Period of 2017-2023 with an Outlook to the Year 2030]. December 2016. In Czech available online: https://www.mdcr.cz/getattachment/Media/Media-a-tiskove-zpravy/Koncepce-nakladni-dopravy-pro-obdobi-2017-%E2%80%93-2023-r/Koncepce-nakladni-dopravy.pdf.aspx . p. 86.

Ministerstvo dopravy [Ministry of Transport][77] from the year 2015 or the *Národní akční plán pro chytré sítě (NAP SG)* [National Action Plan for the Smart Grid (NAP SG] by the Ministerstvo průmyslu a obchodu [Ministry of Industry and Trade][78] from the same year.

The discussion of legal issues related to the smart cities and the appropriate policy approach is in an early stage, there is, however, a number of activities, primarily on the regional and municipal level, in pursuit of strategic and organisational approach. Several major Czech cities are currently working on framework documents for strategy towards becoming a smart city. Participation in national and international cooperation bodies is increasing. The governmental level short term regional development policy documents so far do not hold the smart city development for a priority issue. There is, however, a project for Ministerstvo pro místní rozvoj ČR [Ministry for Regional Development of the Czech Republic] that is aimed towards developing a methodology for smart city development.[79] The most contentious legal issues with regard to smart cities deal with the protection of privacy and personal data, safety and cyber security, as well as availability of open data.

Question 4.4.

In the Czech Republic, there was no new law enacted in connection with the Google Spain decision.

The Office for Personal Data Protection issued in cooperation with SPIR[80] a recommendation for data subjects concerning the right to be forgotten after the Google Spain decision.[81] This document is not binding in any way. It is aimed to inform data subjects and help them to enforce their rights.

[77] Ministerstvo dopravy [Ministry of Transport]. *Akční plán rozvoje inteligentních dopravních systémů (ITS) v ČR do roku 2020 (s výhledem do roku 2050)* [Action Plan for the Development of the Intelligent Transport Systems (ITS) in the Czech Republic until the Year 2020 (with an Outlook to the Year 2050)] 27.3.2015. In Czech available online: https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/ap-its-zakladni-dokument.pdf

[78] Ministerstvo průmyslu a obchodu [Ministry of Industry and Trade]. *Národní akční plán pro chytré sítě (NAP SG)* [National Action Plan for the Smart Grid (NAP SG] February 2015. In Czech available online: https://www.mpo.cz/assets/cz/energetika/elektroenergetika/2016/11/Narodni-akcni-plan-pro-chytre-site.pdf

[79] David Bárta *Metodika Konceptu inteligentních měst* [Methodology for the concept of intelligent cities]. Centrum dopravního výzkumu [Centre for transport research]. 2015. In Czech available online: http://www.strukturalni-fondy.cz/getmedia/9c597c78-8651-43a8-8d94-bc9f19da74c5/TB930MMR001_Metodika-konceptu-Inteligentnich-mest-2015.pdf

[80] SPIR is an Association for Internet Development – a professional association connecting companies with internet oriented business, including the Czech web search engine operator Seznam.cz.

[81] The recommendation is available in Czech online on the web page of the Office for Personal Data Protection: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=12185.

Unfortunately, there are no available statistics concerning number of complaints brought before the data protection authority.

There is no recorded case, in which the court would consider the right to be forgotten. Therefore, unfortunately, it is not possible to assess the question further in detail.

However, there is one case, in which the right to be forgotten was used as a part of argumentation. In the decision of the Regional court in Brno[82] No. 70 Co 228/2015-38 from 7 November 2015, the Court stated that it will not order an injunction to remove content allegedly breaching right for privacy and personal data protection of the plaintiff from the Internet. The plaintiffs tried to use the Google Spain decision in their argumentation, but the Court decided against their claim for two reasons: A) it is not possible to grant as an injunction a claim, which is also claimed for the final decision; B) the content was online since 2007, therefore it was not reasonable to use the preliminary ruling for its removal, since any possible harm was probably already done.

[82] In this case the court acted as the court of appeal.

ESTONIA

Professor Tanel Kerikmäe* • Sandra Särav**
Evelin Pärn-Lee*** • Kärt Salumaa****
Kari Käsper***** • Agnes Kasper******

1. Internal Market and electronic commerce : Internet and e-commerce
1.1. Electronic Commerce, liability of Internet intermediaries

Question 1.1.1.

The concept of information society services, service provider, as well as the liability of an intermediary are set forth in Estonian Society Services Act (*Infoühiskonna teenuste seadus*) [1]. Section 8 of the Estonian Society Services Act introduces Article 12 of the Directive 2000/31/EC on electronic commerce almost word by word. Therefore *mere conduit* by the service provider does not trigger the liability, provided the service provider does not initiate the transmission, or select the receiver of the transmission and does not select or modify the information contained in the transmission. National rules related to caching, hosting and no general obligation to monitor[2] follow also almost word by word relevant provisions of the directive provided by Articles 13, 14 and 15.[3]

* Head of Tallinn Law School, Tallinn University of Technology.
** Junior researcher at Tallinn Law School, Tallinn University of Technology.
*** Junior researcher at Tallinn Law School, Tallinn University of Technology.
**** Junior researcher at Tallinn Law School, Tallinn University of Technology.
***** Lecturer at Tallinn Law School, Tallinn University of Technology.
****** Guest Lecturer at Tallinn Law School, Tallinn University of Technology.

[1] RT I 2004, 29, 191.

[2] As set out in sections 9, 10 and 11 of the Society Services Act.

[3] Given report on behalf of Estonian rapporterurs has been drafted under the Personal Research Funding Project funded by Estonian Research Council: The assessment of Estonian national e-government services system in the context of EU's legal framework of Digital Single Market.

Estonian case law on internet intermediary liability is rather limited and relates mostly to online news portals and the means for readers to comment the news published by the portals. Already in 2009 the Estonian Supreme Court stated[4] that online news portals who provide content services and not passive intermediation service cannot be exempted from the liability. Online portals who provide online commentary possibilities are engaged in activity which nature is not merely technical, automatic, and passive, thus they cannot claim of having no knowledge or control over the information transmitted. The Supreme Court ruling has been followed by a number of decisions by lower courts[5] in which they consider online news portals which provide also commentary possibilities providers of content services. Although not author of the comments the online news portal are considered publisher of such comments as held financially interested in publishing comments (as the revenue of sale of advertisement depends on the number of comments). According to the case law online news portals control the information stored in the commentaries, they control the transmission, storage as well as deletion thereof. Because of that they cannot be exempted from the liability of the intermediary service providers. The separate discussion has been related to the private blogs – Estonian Supreme Court asked preliminary ruling related to the scope of liability of false information in internet. By one of the latest judgements by Tallinn Circuit Court in 2014, a statements in personal blog that were considered false, the court obliged the blogger to remove the information from the blog and make a clear statement that his former claims were not correct.

Question 1.1.2.

Pursuant to L'Oréal v eBay, C-324/09 *Article 14 (1) of Directive 2000/31/EC (E-Commerce directive) applies to the operator of an online marketplace where the latter has not played an active role allowing it to have knowledge or control of the data stored.* Respectively, as the result of it, if the operator has played an active role in the promotion or sale of the trade marked goods or gained knowledge of facts or circumstances of illegal actions, such as for example trademark infringement, the latter can no longer hide behind the *hosting* defense as set forth in Article 14 of the E-Commerce Directive.

There are no national cases on the issue of liability of an online marketplace operator in connection to trade mark infringement. Therefore it is not possible to comment from the national point of view if the test established by CJEU creates any difficulties in interpreting or applying the relevant EU or national regulation.

[4] 3-2-1-43-09 Leedo vs Delfi.

[5] Such as for example Tallinn Circuit court ruling 2-10-46710 from 27.06.2013, Narva county court 2-15-6204 from 30.09.2015, Tartu Circuit court ruling 2-15-6204 from 29.02.2016.

We agree with the CJEU that the mere fact that an online marketplace operator stores offers for sale on its server, sets the terms of its service, is remunerated and provides general information cannot result in liability exemption provided in E-Commerce Directive being declined[6]. If the activity of the operator of an online marketplace is purely technical, automatic or passive with no knowledge or control over the data stored, relevant person should be ensured exclusion of liability[7]. On the other hand, if the role of the online marketplace operator is active in a way that it gives the latter knowledge or control over the data stored, the liability exemption should not be ensured. But how to handle cases in which there is only some control over the date, also when the conduct of the online marketplace operator cannot be described as fully neutral or technical. For example, the service provider always has the possibility to turn the service off, or delete all data. Will this give it control sufficient to claim that its conduct is not passive or neutral.

Each case has its context, and when considering the applicability of the test for liability as set forth in L'Oréal v eBay, C-324/09, has to be carefully considered before liability exemption can be denied or confirmed. However, it should be ensured that no different rules apply to businesses conducted in traditional way (e.g. in store or marketplace) or through e-commerce.

Question 1.1.3.

According to Article 14 (1) b) of the E-Commerce Directive the liability exemption applies on the condition that the service provider upon obtaining knowledge or awareness of illegality acts expeditiously to remove or to disable access to the information. The same is provided in Section 10 (1) 2) of the Estonian Society Services Act.

There is limited case law on national level on the applicability of the above regime. There are few cases in which it is recorded that the service provider has removed data after relevant notice of the data subject. These relate to comments made in the commentary provided by online news portals. In practice, it is common that the online portals which provide commenting possibility prescribe in their terms and conditions that they should be notified of any inappropriate comment. And if so they remove or limit access to the relevant comment.

Based on the above, as there is little practice on the regime, it is not possible to comment if there are areas in which the regime of notice-and-take-down works better than in the others.

[6] See L'Oréal v eBay, C-324/09, p 115.

[7] See Google France and Google, Joined Cases C-236/08 to C-238/08, p 114.

From theoretical point of view, however, the regulation is to some extent vague. It is not clear if the liability exemption requires the service provider to remove or disable access on the first relevant notice, or shall the service provider wait until the data claimed to illegal, is considered so by a court ruling. Clause 46 of the preamble of the E-Commerce Directive indicates that the removal or disabling of access must be done in the observance of the principle of freedom of expression and of procedures established for this purposes at national level. Also, that the E-Commerce Directive does not affect the member states possibility to establish specific requirements for to be obeyed before removal or disabling access. Estonia has not established any such requirements.

Question 1.1.4.
The national court practice in the field is rather limited. When confronted with injunctions it is very likely that the national courts will refer to the case law of European courts.

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.
The principles set out in Directive 1999/44/EC on the sale of consumer goods and associated guarantees have been incorporated into Estonian legal System. According to Section 222 of the Law of Obligations act, *if a thing does not conform to the contract, the purchaser may demand the repair of the thing or delivery of a substitute thing from the seller if this is possible and does not cause the seller unreasonable costs or unreasonable inconvenience compared to the use of other legal remedies considering, inter alia, the value of the thing, the significance of the lack of conformity and the opportunity for the purchaser to acquire a thing which conforms to the contract from elsewhere without inconvenience.* The seller is provided with the right to choose if to instead of repairing the thing, to deliver a substitute[8]. If the seller chooses to replace the defective thing with a new one, the latter can claim return of the defective replaced thing[9]. Any costs related to repair or substitution must be borne by the seller[10]. In case the purchaser requires repair and the seller fails to do it within a reasonable period of time, the purchaser may organize repairing and claim compensation for any reasonable costs incurred thereupon from the seller[11]. It

[8] Section 222 (1) of the Law of Obligations Act.
[9] Section 222 (3) of the Law of Obligations Act.
[10] Section 222 (4) of the Law of Obligations Act.
[11] Section 222 (5) of the Law of Obligations Act.

is, however, important to note that the claim to repair or substitute a defective thing must be done at the same time with the notice on defects. If not done at the same time the purchaser loses the right to require the repair or delivery of a substitute, unless the seller is not acting in good faith[12].

Guarantee is prescribed in Sections 230 and 231 of the Law of Obligations Act. According to Section 230 (1) *a guarantee* against defects is a promise made by a seller[13] to replace or repair a sold thing without charge or for a charge and under the conditions prescribed in the guarantee or advertising, or to ensure in other ways the compliance of the thing with the conditions prescribed in the guarantee or advertising whereby the purchaser is given a broader warranty than that provided by law. Pursuant to law it is presumed that the guarantee covers all defects that appear during the warranty period[14].

Additionally, Section 231 of the Law of Obligations provides specification for guarantee in case of consumer sale. According to this, *in* consumer sale the guarantee shall set out, in a manner understandable to the consumer, information on the guarantee and the procedure for exercising the rights under it. A guarantee must provide inter alia, (i) the name and address of the guarantor, (ii) the person to address to exercise the rights arising from the guarantee, (iii)the rights granted to the consumer by the warranty, (iv) the procedure for exercising the rights arising from the warranty, (v) the warranty period, (vi) the scope of the guarantee and (vii) an explanation that, in addition to the rights arising from the guarantee, the consumer has other rights arising from law[15]. Also, the consumer must have the possibility to examine the conditions of the guarantee before entering into sale contract[16]. Further or, in case of consumer sale, it is presumed that the guarantee ensures the purchaser the right to demand free of charge repair or substitution of the defective thing, whereas in case of substitution new warranty with the same duration as the original will start upon replacement, and when repaired the guarantee period is automatically extended by the length of the period of repair[17].

Question 1.2.2.

In our opinion the Directive proposal is a big step forward and most definitely will serve for clearer rules, especially considering that not only businesses transact globally, but also consumers buy things on global markets. If the Directive proposal provides for the best possible rules enabling the achievement of a genuine

[12] Section 222 (6) of the Law of Obligations Act.
[13] Previous seller or producer.
[14] Section 230 (3) of the Law of Obligations Act.
[15] Section 231 of the Law of Obligations Act.
[16] Section 231 (2) of the Law of Obligations Act.
[17] Section 231 (4) of the Law of Obligations Act.

digital single market, can, however, yet not be answered. Mostly, because the law makers seem to be always a step behind the technological developments, thus it is most probable, that not all possible e-commerce means are covered with the new directive. One of the highlighted priorities of Estonia in the context of its EU presidency is : "developing cross-border e-commerce and e-services for the benefit of consumers, producers and businesses"[18]. As to the domestic market, currently, there are ca 2000 e-shops registered in Estonia, but it is also significant that 33% of estonians buy goods through e-platforms from abroad.

Question 1.2.3.
Please see the answer above.

Question 1.2.4.
Considering that e-commerce takes place cross borders harmonized rules on consumer protection are indispensable. Whereas the beneficiaries are not merely the consumers, equally benefit the business who are engaged in e-commerce. Making sales on the digital single market is more transparent and risks lower if the rules are harmonized. Considering, however, that the digital single market does not expand outside the EU, it should be duly considered how to provide consumer protection on the transactions beyond EU digital single market.

Question 1.2.5.
In general the rights of consumers as set out in relevant EU consumer protection law seem to be safeguarded when making contracts, regardless of if made in ordinary way or online. But can the consumer effectively claim remedy or apply for guarantee of a defective service or item provided by an online platform seated outside the country of residence of the consumer. When the aim is to have a fully functioning digital single market, it should also *inter alia* safeguarded that the consumers can effectively exercise its rights in the country the make service provider is seated. One of the priorities of Estonia (within the EU presidency) is to lead the discussion that would remove the geo-blocking based restrictions and harmonise the rights and liability in the digital market. For Estonia, the topic of boosting the development in the field is also relevant as the government "hopes digital innovation will turn it into a global superpower in e-commerce by offering foreigners e-residency IDs, and opening the door to doing business online throughout the European Union"[19].

[18] See: https://www.employers.ee/en/uncategorized-en/estonian-presidency-of-the-council-of-the-european-union/#priorities.
[19] Maris Hellrand, Mary Sibierski, Estonia Wants To Be Come A Global Superpower Through E-Commerce, Business Insider, 2014.

Question 1.2.6.
Not to our knowledge. There have been cases of bankruptcies. For example, in 2015, when a quite popular company (selling furniture online) had to file bankruptcy after it has been accused by ca 200 clients (to the Consumer Protection Agency) that it has no further capacity to fulfil orders. The Consumer Protection Agency provides updated blacklist of e-shops that have had continuous problems in terms of consumer protection regulations (https://www.tarbijakaitseamet.ee/et/ametist/e-poed-kes-ei-taida-seadusest-tulenevaid-noudeid). At the same time, the list of secure web-shops is available for customers (https://e-kaubanduseliit.ee/kvaliteedimark/kvaliteedimargiga-e-poed/) by Estonian e-commerce union.

Question 1.2.7.
Considering that the question reads *do you consider it necessary/useful to expand the scope of the rules on Business to Consumers (B2C) to Business to Business (B2B),* our opinion is affirmative, it would be utmost useful to expand the rules also to B2B transactions. There seem to be no clear reasons why there should be different set of rules to B2C and B2B transactions. At least to SMEs and micro-businesses, it would be a tool to provide them sufficient protection against unfair trading terms.

1.3. Geo-blocking

Question 1.3.1.
During the time of preparing the answers to given report, it is only possible to rely on the draft text of the Regulation. Therefore, as far as the draft text is concerned, the opinion is that the proposed Regulation is seeking to avoid conflict with the Regulation 1215/2015 (Brussels I). In the draft regulation addressing unjustified geo-blocking, the Article 1 (5) specifically lays down that the proposed regulation does not "affect acts of Union law concerning judicial cooperation in civil matters." Specific reference is made to Regulation 1215/2015 article 17 (1), setting forth that „[c]ompliance with this Regulation shall not be construed as implying that a trader directs his or her activities to the Member State where the consumer has the habitual residence or domicile," within the meaning of point c of the aforementioned Article of Brussels I.

Nevertheless, it still may be questionable whether the two regimes of the respective draft Regulation and the Regulation in force can function properly if they have to be isolated from each other. To be more specific Brussels I regulation has in place the specific rules in order to protect the consumer, as the weaker party of the contractual relationship. Namely, the Brussels I sets forth that the consumer can only go to court against the trader in the former's domicile; and that proceedings may only be started against the former in his / her domicile. The current form of the proposed regulation leaves it unclear how to evaluate

that a certain activity by the trader means that she or he is directing activity towards a certain Member State, as opposed to merely following the requirements of the proposed regulation, i.e., the readiness of the trader to engage in contractual relationship with consumers from any Member State (Article 4). The official standpoint of Estonia is that in current form of the proposed regulation, it is rather convenient for the trader to rely on the fact that he or she is merely fulfilling the obligations coming from the regulation, and thus set aside the rules set forth in both Rome I and Brussels I regulations for the protection of the consumer. Thus, it should be of utmost importance to put in place a wording that allows unequivocal interpretation and to offer legal certainty for both traders and consumers, especially when it comes to the question of jurisdiction and the overlap with the Brussels I regulation.[20]

1.4. Questions related to the collaborative economy

Question 1.4.1.

Estonia has been advertising itself as a country which avoids premature legislation. Therefore, generally, the pre-existing legal framework covers the activities of collaborative economy service providers / business models.[21] However, a few aspects still need to be covered by legislation in one way or another. The main challenges can be divided into three categories:

1. *Taxation issues* – the existing legal framework covers all forms of business models and all sectors. Nevertheless, there is no specific legislation applicable to service provision between natural persons. Therewith, one can also raise the questions of fair declaration of taxes. However, with reference to taxation matters, Estonia also has a success story to present. Since 2015, rideshare drivers can declare their income through a prefilled form provided by the Tax and Customs Board of Estonia.[22] Additionally, on June 14, 2017, the Parliament passed the so-called rideshare bill, that equalises the ride sharing service with traditional taxy service providers and gives them tantamount rights and obligations.[23] The main change in law lies in

[20] Estonian Government official position can be accessed in Estonian: http://eelnoud.valitsus.ee/main#lTWNLesH

[21] See also the Technopolis Group study on the sharing economy in Estonia, available in Estonian, executive summary available in English: https://www.mkm.ee/sites/default/files/lopparuanne.pdf

[22] See for instance, the Estonian Tax and Customs Board Press Statement on increase of declarations from 2015-2016, available in English at: https://www.emta.ee/eng/income-declared-through-uber-and-taxify-has-overwhelmingly-increased

[23] The amendments to the existing public Transport Act will come into force on November 1, 2017. We have now also translated the Estonian text of the Public Transport Act. The paragraphs that are

the fact that the ride sharing providers are not regulated separately, but rather the existing taxi service requirements are softened.

2. *Contractual relations* – there is some legal uncertainty as to which form of contractual relationship is applicable in certain circumstances (e.g., employment contract, contract of services). For instance, there is no regulation on online platforms, and thus, if we take the cases of services that are provided through and online intermediary, the responsibilities between a service provider (the intermediary / platform) are unclear.
3. *Consumer Protection* – as the online platforms are not specifically regulated in Estonia, it raises some concerns from the perspective of consumer protection. E.g., in relation to the information on quality and price formation of the service; to whom to turn to in case of a complaint, etc. There is no assurance in terms of liability. The application of the Estonian Consumer Protection Act is limited to sale, or marketing in any other manner, of goods or services to consumers *by traders*, who are acting "for purposes related to their business or professional activities"; hence meaning that in cases where the other party is not a trader within the meaning of the Act, there is no contractual relationship between the service provider and the consumer.[24]

Question 1.4.2.

The market study on collaborative economy in Estonia[25] indicates that the collaborative economy rather creates new market needs, attracting the customers who previously did not use such services (e.g., price too high, inconvenient to consume, etc). However, the results of the study show that this varies in different sectors. The biggest effect on the traditional market was seen in the accommodation sector. Positive effect was on the financial market, where the sharing economy platforms address foremost a target group whose needs are not satisfied by commercial banks – this means that the new collaborative economy service providers create a new market, which, in turn, boosts competition.[26]

Question 1.4.3.

There are no requirements for offering collaborative economy services, i.e. there are no specific market access requirements to collaborative economy service providers.

regulating taxis are in the chapter 10. Link to the English version is here:https://www.riigiteataja.ee/en/eli/520092017001/consolide

[24] See §§1-2 of the Consumer Protection Act. Available in English at: https://www.riigiteataja.ee/en/eli/521082017004/consolide

[25] Supra nota, 23.

[26] Ibid.

Question 1.4.4.
There are no legal challenges pending or decided known to the authors at the time of the writing of current report. In fact, the Consumer Protection Authoritu of Estonia does not have the legal right to interferece with the dispute between the service provider and the consumer, insofar as the Consumer Protection Act is only applicable to trader-consumer contractual relations, and if, for instance, the accommodation service provider is not a trader within the meaning of the act, the Consumer Protection Auhtority cannot conduct surveillance over such contractual relations.

Question 1.4.5.
The there is no such concept as a "peer" in Estonian legislation (i.e. private individual offering services on an occasional basis). Estonian tax legislation differentiates between service providers based on whether they provide those services as natural persons or legal persons. Pursuant to the Consumer Protection act, trader means "a natural or legal person, including a legal person in public law, who acts for purposes related to their business or professional activities."[27] See also 1.4.1 (3). However, this differentiation is a general one, which does not only apply to the the collaborative economy.

Question 1.4.6.
In a way, the peer-to-peer services market is largely begging for and heavily relying on self-regulatory approach. Take for instance, ride sharing with Uber, Taxify, etc. The driver rating system contributes to consumer choice-making. Therefore, in a way online rating and review systems can contribute to overcoming lack of information about individual service providers. Nevertheless, they can also impede market access to newcomers, for instance, in case of Airbnb accommodation service providers or consumers who have not accessed the platform before and therefore do not currently have any rating. Thus, from yet another angle, the rating systems are also creating room for distrust based on unnecessary scepticism, i.e., the service-provider merely has not been rated yet. Therefore, such tools may provide to be useful; however, they should not exhaust the list of appropriate (regulatory) tools.

In order to encourage to consumers to use collaborative economy services, certain commonly understandable principles must be adopted, e.g., we can see in the case of Estonia that the Consumer Protection Authority does not have a legal standing in such relations. Nevertheless, the market should not be heavily

[27] Estonian Consumer Protection Act. §2 2). Available in English at: https://www.riigiteataja.ee/en/eli/521082017004/consolide

regulated, as this serves contrary to the purpose of the collaborative economy and could hinder its prosperity to begin with.

2. Digital media

Question 2.1.
According to Section 4 of the Media Services Act, registered media services are divided into two main categories, Television service and on-demand audiovisual media service, whereas audiovisual commercial communication and similar services that do not compete with television service do not require any form of registration. The explanatory notes of the Media Services Act clarify that internet media, online newspapers and other new forms of media fall outside the scope of the law.[28] The Technical Surveillance Authority, the regulatory authority of Estonian media services, has considered the option to require larger news portals to register as on-demand audiovisual service in the Register of Economic Activities[29], however currently there are only three undertakings entered in the register in this category and all of them provide video rental services.

Question 2.2.
The new proposals in the AVMS directive would bring video platforms (such as YouTube) together with other sites such as Facebook, Twitter, etc, (which also have significant video sharing capabilities). Extension of the scope of application beyond the socially most sensitive problems would impose disproportionate burden on media service providers (monitoring) that could potentially affect diversity of online media, erode freedom of speech and undermine the competitiveness of European providers. The harm caused by commercial communications in self-regulating audio-visual platforms is potentially lesser than in case of broadcasting, because the former are highly diffuse hence intervention may not be justified on grounds of proportionality or even necessity.

Question 2.3.
The only instance when Technical Surveillance Authority contacted another Member State's regulator (UK) was about a programme broadcasted by REN TV Estonia on the 5th December, 2015, where there was a suspicion that it had contained incitement to hatred based on nationality. The UK regulator demonstrated excellent cooperation with the Estonian TSA and found no violation of rules, however the case showed that the process of thorough analysis can take

[28] Media Services Act explanatory notes.
[29] Vakrõõm, Tais, Piiriülese Audiovisuaalmeedia Taasedastamise Pirramise Õiguspärased Võimalused, MA thesis, Tartu University, 2017. p.5.

long time, hence the timeframe set by Section 3 (2) d) is unreasonably short and that target country's lack of jurisdiction over cross-border media services is an important shortcoming in the regulatory framework.

Other problems that originate from outside the EU are described for example in Yearbooks of the Estonian Internal Security Service, which regularly discuss manipulative Russian media projects targeting Estonia.[30] See also answers to 2.4 and 2.5.

Question 2.4.

Independence of media regulators is a right step. Recent political developments in some Post Soviet and Eastern European countries have shown that regulators must be free from government interference. Such independence would help the like minded regulators to converge together and would facilitate the creation of the single market without any extraneous political pressures. The AVSMD provisions about independence and role of media regulators continue to be relevant and the same approach should be followed in the revision. Yet it is the definition of roles of authorities that raises concerns[31]. In Estonia national security considerations prompted discussion about creation of *flexible* and effective mechanisms to ensure cooperation between media regulators to tackle manipulative propaganda.[32] Closer cooperation, including the creation of a European database of media services, would remove possibilities of „forum shopping" and contribute to the better functioning of the single market. Another approach may be to reconsider basis of jurisdiction and take analogy from the field of collection of digital evidence, where a persons actual „access and control over data" is a factor that can be taken into account and may even replace the territoriality principle[33].

Question 2.5.

Most covered and recurring themes are propaganda and hate speech, however the discussions appear to be rather political than legal in terms of broadcasting laws. We are not aware of relevant court cases, however Estonia has been criti-

[30] Yearbooks available at https://www.kapo.ee/et/content/aastaraamatu-v%C3%A4ljaandmise-traditsiooni-ajalugu-ja-eesm%C3%A4rk-0.html

[31] AVSMD consultations in Estonia, 2015, Q&A.

[32] See for example 19.05.2015 press release from Technical Surveillance Authority „The latest developments in Eastern Europe and the conflict around Ukraine has demonstrated that some foreign broadcasters are acting as a tool of Russian propaganda in the Baltic states and these target states need to defend themselves against the manipulative propaganda. Yet the AVMSD does not provide effective and flexible possibilities for this." https://www.tja.ee/et/uudised/tja-elektroonilise-side-ulevaade-votab-kokku-i-kvartali-arengud-valdkonnas-3

[33] Gathering of Digital Evidence: National and Transnational Challenges for Law Enforcement and Private Industry, Closed experts and stakeholders workshop, Belgium, 28-29, June, 2017.

cised for inadequate legal framework on incitement to hatred.[34] Section 151 of the Penal Code provides that activities which publicly incite to hatred, violence or discrimination on the basis of nationality, race, colour, sex, language, origin, religion, sexual orientation, political opinion, or financial or social status if this results in danger to the life, health or property of a person is punishable by a fine of up to three hundred fine units or by detention[35]. Without court practice on this Article in any context, it is difficult to predict how it would be applied in relation to broadcasting laws.

As to propaganda, Estonian media reflected on the Russian Sputnik channel's plans to start Estonian language broadcasting and recruiting local journalists. While Sputnik is considered as a propaganda tool of Russia, politicians are *skeptical about imposing limitations* in such cases and see the solutions in awareness raising.[36] Considering that this problem is not unique to Estonia, but affects Europe as a whole as well as several individual Member States to a great extent, it seems reasonable to take steps towards facilitating cooperation among Member States and European-level awareness raining.

Question 2.6.
We are not aware of such initiatives.

Question 2.7.
The country of origin principle does not apply to online transmissions of broadcasting organisations.

The *Viasat case* demonstrated that Directive 93/83/EEC remains relevant in practice.[37] The State Court addressed the question what activity qualifies as communication by satellite in the meaning of Section 10 (5) and 10^2 (2) of the Copyright Act[38]. The Court has made direct reference to the corresponding provisions of Directive 93/83/EEC, Article 1 (2)a and c, as well as to the relevant *Airfield* case. It held that the enterprise that makes it technically possible to communicate a work to the public by satellite is merely a technical service provider and does not independently communicate programmes in the meaning of the law, hence for this activity it does not need authorisation from the authors nor pay

[34] CoE – ECRI Report on Estonia, 2015 http://www.coe.int/t/dghl/monitoring/ecri/Country-by-country/Estonia/EST-CbC-V-2015-036-ENG.pdf

[35] Section 151 of the Penal Code.

[36] http://www.err.ee/554957/kross-sputnik-proovib-alternatiivse-toega-risustada-laane-inforuumi

[37] Eesti Autorite Ühing vs Viasat AS, case nr 3-2-1-50-13 of 29.05.2013 and nr 2-11-17594 of 28.02.2014.

[38] Section 10^2 (2) states that „For the purposes of this Act, „communication by satellite" means the act of introducing, under the control and responsibility of the broadcasting service provoder, the programme-carrying signals intended for reception by the public into an uninterrupted chain of communication leading to the satellite and down towards the earth."

them fees[39]. Merely selling decryption devices under the control of television service provider does not make the former enterprise a broadcasting service provider[40]. Hence the defendant does not need a licence from the authors if its activity in communication of a programme to the public is limited to providing tools, the aim of which is to make such communication possible or to carry it out[41]. However, the Court noted that even if primarily the television service provider is deemed to communicate programmes in the meaning of the law, authors' authorisation is necessary for the satellite service provider too, if the latter makes the programme available to a broader public than it was contemplated in the agreement, concluded between the television service provider and authors, on the transmission of the works.[42]

Question 2.8.

Main barrier is the current licencing model that is based on territorial licenses. Estonia has been advocating for ending geo-blocking and have proposed the vision of a 5th freedom, free movement of data in the European Union, hence significantly departing from the traditional legal regimes[43].

Controlling the country of residence of the consumer by the service provider, especially on a regular basis appears to be a disproportionate measure to the aim to be achieved. It can be presumed that in the majority of the cases the country of residence will not change frequently, because it can be considered as a rather exceptional event for everyday people. From Estonia's approximately 1,5 million population less than 30,000 people changed their country of residency in 2016.[44] This amounts to cca 2%, thus it can be expected that controlling whether the consumer have changed residence would be answered positively in the same proportions from all contracts. Allowing private entities to process personal data, especially on a regular bases, in cases where the rights and obligations of the parties in the contractual relationship will not change and the status quo will be kept, goes beyond what is necessary to achieve the goals of the law. Less invasive measure would be to collect information only in those cases, when country of residence is actually changed. For these purposes consumer could be required to notify the service provider (although intuitively this can be ineffective solution) or schemes could be devised creating and involving collective right management organisations for consumers.

[39] Viasat case, para 23.
[40] Viasat case, para 24.
[41] Viasat case, para 27
[42] Viasat case, Para 26.
[43] Estonian Vision Paper on the Free Movement of Data – the Fifth Freedom of the European Union, https://www.eu2017.ee/sites/default/files/inline-files/EU2017_FMD_visionpaper.pdf
[44] Statistics Estonia, Estonia's net migration was positive in 2016, 23 May 2017 – news release no 59.

3. Digital infrastructures

Question 3.1.

In Estonia, no specific national rules regarding net neutrality exist at the time of the writing of the report. The Electronic Communications Act only includes requirements of *technological* neutrality of radio frequency allocation plan (§ 9(1[1])), sector-specific regulation of markets of communications services (§ 40 (3)), and overall implementation and compliance with the Act (§ 134 (5)). While not specifically guaranteeing net neutrality, it mentions that the sector-specific regulation of markets of communications services "is to ensure the pluralism of communications service providers, their equal and non-discriminatory treatment by encouraging competition, and the quality and availability to end-users of the provided services."

There is also no specific policy or approach regarding zero-rating, which has not been discussed in the Estonian context. Although zero-rating appears not to be prohibited by law, it appears it is not used in practice by the operators in Estonia.[45]

Question 3.2.

There is no explicit information about Estonia's position regarding the single market for telecommunications networks or services.

In 2009 the Estonian government and telecommunications companies launched jointly the EstWin project, with the aim "to give all residential houses, businesses and authorities a chance to connect to the next-generation broadband network with a transmission speed up to 100 Mbit/s by the year of2018."[46] The project foresees the installation of more than 6000 km of cables, which ensures that 98% of residential houses, businesses and authorities are located closer than 1,5 km from the basic network. The Estonian Ministry of Economic Affairs and Communications and the members of Estonian Association of Information Technology and Telecommunications created the Estonian Broadband Development Foundation in order to manage the project.

Since the project involved state aid, the Commission was informed. In 2010, the Commission approved the aid as service of general economic interest, noting that the "measure will offset a geographical and commercial handicap in the rural areas of Estonia and will enhance the competitive supply of high speed broadband services across the area."[47] EU structural funds are used as funding source for the state funding of the project (85%).

[45] http://ec.europa.eu/competition/publications/reports/kd0217687enn.pdf

[46] Objectives of the Estonian Broadband Development Foundation. The website of Estonian Broadband Development Foundation. http://www.elasa.ee/index.php?page=122

[47] State aid N 196/2010 – Letter to the Member State, 20 July 2010, available at http://ec.europa.eu/competition/state_aid/cases/236358/236358_1183816_63_2.pdf

Next-generation broadband (EstWin project) is also one of the key priorities in the Digital Agenda 2020 for Estonia.[48]

Question 3.3.
Spectrum management is regulated under the Electronic Communications Act. There have been no specific legal issues with spectrum management. The institution responsible for spectrum management is Technical Regulatory Authority that also deals with other aspects of regulation of communications services, including competition issues.

Question 3.4.
No, such issues have not been raised in the public discussion, nor has there been any legal challenges. The institution responsible for spectrum management is Technical Regulatory Authority that also deals with other aspects of regulation of communications services, including competition issues.

4. Data in the digital economy

Question 4.1.
When it comes to the General Data Protection Regulation (GDPR) and the legislative side of the implementation, then the responsible ministry for the implementing legislation is the Estonian Ministry of Justice. The Ministry of Justice, with this new planned piece of legislation, is implementing the GDPR and also transposing the so called "police directive" (directive 680/2016) which is another part of the European Union's personal data protection reform. Therefore two pieces of European Union legislation will be covered with one new general legal act in Estonia: new Personal Data Protection Act (*isikuandmete kaitse seadus* in Estonian) will replace the old one. This new legal act is expected to come into force before the 25th May 2018 which is the application date for the GDPR (art 99 of the GDPR).

The new Estonian Personal Data Protection Act will probably (it's not published during the writing of this text) consist of the aspects that are domestically essential to cover aspects left unspecified or that need specification by the GDPR (see GDPR recital 8) and provisions transposing "police directive". At the time of writing this text, it is quite certain that the new Personal Data Protection Act will also include general provisions laying down the overall ground for the national law in the field of personal data protection, provisions necessary for the activities and operation of the Estonian national Data Protection Authority

[48] Ministry of Economic Affairs and Communications, Digital Agenda 2020 for Estonia. https://www.mkm.ee/sites/default/files/digital_agenda_2020_estonia_engf.pdf

(DPA), *Andmekaitse Inspektsioon*, and special Chapter for the implementation of Chapter 9 of the GDPR (specific processing situations including *e.g.* data processing in the light of freedom of expression and information, public access to official documents, in the context of employment, processing of the national identification number etc). Another voluminous and sizeable part of the new legislation in the field of personal data protection will definitely be the numerous amendments of special laws which include many specific situations of the processing of personal data. These numerous amendments will be made taking into account the new European Union legislation regarding personal data protection.

What is more, not only the Estonian Ministry of Justice is making preparations for the implementation of the GDPR and the data protection reform overall. Because GDPR affects both public and private sector, the increase of interest from the private sector is also noticeable. It's in the best interests of the private sector to avoid sanctions and fines which have received a lot of notice since the adoption of the GDPR. To be a great partner to both, private and public sector, and to rise awareness, Estonian National DPA has created a special informative and explanatory column on their webpage (www.aki.ee) focusing especially on the personal data protection reform and topics related to that.

When it comes to the General Data Protection Regulation (GDPR) and the legislative side of the implementation, then the responsible ministry for the implementing legislation is the Estonian Ministry of Justice. The Ministry of Justice, with this new planned piece of legislation, is implementing the GDPR and also transposing the so called "police directive" (directive 680/2016) which is another part of the European Union's personal data protection reform. Therefore two pieces of European Union legislation will be covered with one new general legal act in Estonia: new Personal Data Protection Act (*isikuandmete kaitse seadus* in Estonian) will replace the old one. This new legal act is expected to come into force before the 25th May 2018 which is the application date for the GDPR (art 99 of the GDPR).

The new Estonian Personal Data Protection Act will probably (it's not published during the writing of this text) consist of the aspects that are domestically essential to cover aspects left unspecified or that need specification by the GDPR (see GDPR recital 8) and provisions transposing "police directive". At the time of writing this text, it is quite certain that the new Personal Data Protection Act will also include general provisions laying down the overall ground for the national law in the field of personal data protection, provisions necessary for the activities and operation of the Estonian national Data Protection Authority (DPA), *Andmekaitse Inspektsioon*, and special Chapter for the implementation of Chapter 9 of the GDPR (specific processing situations including *e.g.* data processing in the light of freedom of expression and information, public access to official

documents, in the context of employment, processing of the national identification number etc). Another voluminous and sizeable part of the new legislation in the field of personal data protection will definitely be the numerous amendments of special laws which include many specific situations of the processing of personal data. These numerous amendments will be made taking into account the new European Union legislation regarding personal data protection.

What is more, not only the Estonian Ministry of Justice is making preparations for the implementation of the GDPR and the data protection reform overall. Because GDPR affects both public and private sector, the increase of interest from the private sector is also noticeable. It's in the best interests of the private sector to avoid sanctions and fines which have received a lot of notice since the adoption of the GDPR. To be a great partner to both, private and public sector, and to rise awareness, Estonian National DPA has created a special informative and explanatory column on their webpage (www.aki.ee) focusing especially on the personal data protection reform and topics related to that.

Question 4.2.

As an answer to this question, it is not possible to demonstrate any results of any concrete analysis carried out in Estonia in this area yet because no such thorough analysis exists at the moment of writing this text. However, the representatives of the Estonian Ministry of Justice have been engaged to the discussions which have taken place in the banking, finance and insurance sector and have facilitated the process to develop new approaches originating from the personal data protection reform and GDPR linked to the questions related to consent, data protection impact assessments and the principle of privacy by design and by default.

One of the problem that might probably rise in Estonia and that is related to the implementation of GDPR and the data protection reform, is the proportionally large number of SMEs compared to the amount of big businesses and enterprises operating in Estonia. Estonian national DPA is facing a data protection challenge to raise awareness among SMEs and start-ups and get them to comply with the new data protection legal framework. So far Estonian National DPA has published articles in mainstream media channels and also attended start-up events such as Garage48 which is one of the top events for start-ups in Estonia.

To sum it up, there are no statistical data or analyses yet at the time of writing this text how businesses in Estonia are adapting to the new requirements of the GDPR. However, active work is going on the national level to achieve the high level of awareness.

Question 4.3.
The underlying idea of functioning of the aforementioned concepts is data, in terms of M2M, automated cars' IoT, etc, more specifically we refer to non-personal data. The precondition for effective implementation of such systems is the free flow / free movement of the data granting the function of, and generated by such concepts. Estonia is a strong protagonist of digital and technological developments; and is promoting (especially during the Council of the EU Presidency, second half of 2018) within the EU that, for the sake of a true data economy, data itself needs to become the fifth freedom of the EU.

During the Council Presidency, Estonia adopted a Vision Paper on the Free Movement of Data, setting forth, inter alia, that, "[i]n order to make the fifth freedom a reality, Europe should focus on:

- the removal of any unjustified data localisation requirements to non-personal data to remove digital borders and enable cross-border business;
- promoting cross-border exchange of public administration data on the basis of the once-only principle to serve citizens and business by cutting red tape; and
- creating clear rules on data access and portability to remove legal uncertainty and to promote competition and innovation."[49]

This means that during the Council Presidency, Estonia is leading the EU-wide political debate on the September 13 European Commission proposal on a regulation for free flow of data.[50] The underlying idea is that non-personal data should move across borders just as personal data can move under the General Data Protection Regulation.

Question 4.4.
The "right to be forgotten" or the right to be delisted is not *expressis verbis* written into Estonian domestic legislation. However citizens are allowed to use that right in Estonia when relying on the ECJ case of *Google Spain*. According to the feedback of Estonian national DPA, there is an increase of the use of the "right to be forgotten". Estonian DPA is accepting these complaints on the basis of § 21 (right of the data subject to demand termination of processing of personal data and correction, closure and deletion of personal data) of the currently existing Personal Data Protection Act. However, no separate record is being kept by the

[49] Estonian Vision Paper on the Free Movement of Data – the Fifth Freedom of the European Union, available at: https://www.eu2017.ee/sites/default/files/inline-files/EU2017_FMD_visionpaper.pdf
[50] State of the Union 2017: A framework for the free flow of non-personal data in the EU, available at: http://europa.eu/rapid/press-release_IP-17-3190_en.htm

Estonian national DPA about the number of these cases. What is more, no "right to be forgotten" cases have reached to the Supreme Court of Estonia yet.

When it comes to the balance struck between individual's right to data protection and the other interests at stake, then, of course, sensible balance is needed when relying on this right in Estonia. "The right to be forgotten" needs to be balanced when it comes to public's right to information and the author's right to freedom of expression. In general, the data subject doesn't have the "right to be forgotten" or the right to have his/her personal data deleted if there exists a legal ground for this data to be processed in a lawful way. Therefore a data subject doesn't have the right to have his/her data deleted, for instance, from the population register because there exists a lawful basis for processing data in that specific state register.

When exercising the "right to be forgotten", according to the feedback from Estonian DPA, it may be the case that an individual turns to DPA with the application to get his/her data deleted. In a situation like this, the DPA mainly asks the data subject to firstly turn to the data controller and in many cases, this might conclude the case. When the case can't be solved like described earlier and requires the intervention of a DPA, Estonian national DPA intervenes when the case falls under their jurisdiction.

FINLAND

Juha Lavapuro
Tuomas Mylly*

1. Internal Market and electronic commerce : Internet and e-commerce
1.1. Electronic Commerce, liability of Internet intermediaries

Question 1.1.1.
There haven't been any particular difficulties that Finnish courts have confronted in relation to intermediary service providers, while laying down rules or deciding cases. As far as we know, the approach of the Finnish courts does not differ much from the practices in other Nordic countries being EU Member States. The basic definitions and delimitations are now defined in Chapter 1 of the Information Society Code (Law 607/2015). The definitions are largely the same as in the Ecommerce Directive. However, the Information Society Code is more detailed regarding the obligations and safe harbours of Internet intermediaries.

Question 1.1.2.
In L'oréal v. Ebay, the CJEU interpreted Article 14(1) of the E-commerce Directive, which establishes a so-called safe-harbour for ISPs. The E-commerce Directive does not harmonize the grounds of liability of ISPs, but merely the grounds for immunity from liability as defined in national law. That is, the CJEU could not put forward a comprehensive test for liability, but only for immunity standard from liability. This means that even if the ISP does not fall under the safe-harbour (immunity), it may not be liable under national law. Nevertheless, the relevant safe-harbour test might also include elements that are typically analysed

* Both professors at the Faculty of Law, University of Turku. We are thankful for Law and Information Society Masters' Degree Programme students Vera Fovet and Tero Poutala for research assistance.

under the liability regimes as defined in national laws. Moreover, like in the *GS Media* case (concerning liability for linking), the CJEU could address issues typically considered under secondary liability (such as previous notices and intent) as issues falling under primary liability. In both these ways, the CJEU could through its case law further harmonise the liability regime as concerns ISPs and bring liability issues under its own interpretative competence. The basic test for the safe harbour as defined in L'oréal v. Ebay is relatively ambiguous. The CJEU left much discretion to the national court. It would be preferable if the CJEU / applicable legislation defined the parameters of liability / exemption from liability in more detail. Uncertainty and national variations might lead to unnecessary self-restraint on the part of ISPs and/or excessive claims on the part of intellectual property (IP) owners, and thus for example to potential chilling effects on freedom of expression. With European Court of Human Rights (ECtHR) cases such as *Delfi v. Estonia* and *MTE v. Hungary*, new ways of assessing the liability of the operator are potentially emerging. This however does not necessarily clarify the liability questions as the CJEU and the ECtHR are not engaging sufficiently with the case law of the other court.

Question 1.1.3.

The notice-and-take down constitutes part of the safe-harbour test under the Ecommerce Directive. Thus, it does not determine liability as such, but immunity from liability. The basic conditions of liability are predominantly defined under national laws. The notice-and-take down regime could be distinguished for different types of on-line wrongdoings. For example, child pornography and copyright infringements do not relate to similar background protection interests and should thus be distinguished in terms of ISP liability.

As regards manifest *hate speech and child pornography,* notice-and-take down could be replaced by mere and automatic take-down by the operator, before court order or any other notice. It is already the case in Finland (see Swiss Institute of Comparative Law, 'Blocking, Filtering and Take-Down of Illegal Internet Content', 2015). In these kinds of situations, the operator should still notify the content provider of the takedown. Adequate remedies and mechanisms should be available for the alleged wrongdoer to secure freedom of expression and user rights. These should be regulated in detail on the level of EU law.

In the area of copyright, the current notice-and-take down regime could possibly be replaced by a notice-&-notice regime, as implemented by Canada in their 2010 digital copyright reform. The notice-&-notice regime gives the operator the sole responsibility of acting as a notifying agent, whereas the alleged copyright infringer becomes the only target for action. This would introduce balance to the current regime, which favours the interests of copyright owners. In any case,

adequate remedies and mechanisms should be available for the alleged infringer to secure freedom of expression and user rights. For example, put-back and counter-notification provisions should be at place (following the model of the US DMCA). With recourse to such mechanisms, the alleged wrongdoers could dispute the unlawfulness of their conduct, thus enabling the ISP to maintain the hosting of the content in question if the right holder does not initiate proceedings and establish infringement. It would be preferable to legislate about such rights and mechanisms on the EU-level. However, in the light of the EU Commission's recent copyright proposals, any reforms capable of balancing the rights of copyright owners with other interests do not seem likely.

Moreover, future-oriented orders on ISPs, aimed at prevention of future infringements by others, have become increasingly usual. Costs for the implementation of such measures have often been placed on the ISPs alone. Such future-oriented monitoring and filtering obligations should be clearly and narrowly defined, and where the ISPs have no fault, they should not be solely liable for the related costs of implementing such measures. In the area of trademark counterfeits, the Memorandum of Understanding (MoU) on the Sale of Counterfeit Goods via the Internet (2011) regulates notice-and-takedown. By enabling notifications concerning sellers who generally engage in the sale of counterfeits, it seeks to move away from the specificity of notice as a condition of knowledge relevant for the secondary liability of the ISP. This might increase the risk of collateral damage on the freedom of expression interest and turn the obligation of the ISP towards a future-oriented regulatory function. As the EU is part of the MoU, such concerns should be taken into account in the drafting of such MoUs.

Question 1.1.4.

Finland has detailed legislation concerning injunctions in Section 60 c of the Copyright Act. Finnish courts have issued several times injunctions based on this section, such as in the decision against Elisa Corporation, explained in more detail below (decision 11/41552, 26th of October 2011). According to Section 60 c of the Copyright act, the court may order the service provider acting as an intermediary to discontinue, on pain of fine, the making of the allegedly copyright-infringing material available to the public (injunction to discontinue).

When trying a case the court may, according to section 60 c of the Copyright Act and also upon request of the author or his/her representative, order the service provider acting as an intermediary to discontinue, on pain of fine, the making of the allegedly copyright-infringing material available to the public (injunction to discontinue), unless this can be regarded as unreasonable in view of the rights of the person making the material available to the public, the intermediary, the recipient of the material and the author. When consid-

ering such a request, the court must reserve an opportunity to be heard for both the person against whom the injunction is sought and the person making the allegedly copyright-infringing material available to the public. The order may not endanger a third person's possibilities to send and receive messages. It has been stated in the legal scholarship that Finland is one of the few examples of relatively detailed legislation on the implementation of Article 8(3) of the Information Society Copyright Directive.[1]

Finnish courts have previously often neglected interests other than those of right owners in copyright blocking order cases, in particular (e.g. case IFPI v Elisa). However, due to recent legislative changes in the Finnish Copyright Act, with *travaux preparatoires* (HE 181/2014) emphasizing fuller balancing when imposing obligations on intermediaries, the approach is likely to change. Moreover, the relevant CJEU case law endorses such an approach. There are already indications of such a change in lower court case law in Finland.

However, existing case law is still problematic. Helsinki district court issued an interim injunction to discontinue based on section 60 c of the Copyright Act (decision 11/41552, 26th of October 2011). The decision was issued against Elisa Corporation. Elisa Corporation is one of the biggest companies in Finland providing telecommunication services. The court ordered Elisa Corporation to prevent access to the Pirate Bay site. Elisa Corporation was ordered to delete domain names used by the Pirate Bay, and prevent access to the IP addresses used by the Pirate Bay's service. The court evaluated whether the injunction was unreasonable from the perspective of fundamental rights, namely freedom of speech and copyright owner's right to property. It said that the decision should not interfere more with the making available of material than what is necessary in order to protect copyright.

Helsinki Court of Appeal affirmed the decision (decision number 1687, S 11/3097, 15th of June 2012). The Supreme Court of Finland did not grant parties the right of appeal. There are similar decisions concerning TeliaSonera and DNA corporations (Helsinki District Court, 11.6.2012 H11/48307 and Helsinki District Court, 11.6.2012 H11/51544). These companies also provide telecommunications services. In both cases, the orders concerned Pirate Bay. These decisions have been criticized, as despite the function of the relevant norms being targeted at interim measures, the aim of the proceedings has been permanent blocking. Moreover, such measures could constitute ex ante restriction of freedom of expression, as prohibited by section 12 of the Finnish constitution.[2]

[1] *Savola, Pekka*: Internet Connectivity Providers as Involuntary Copyright Enforcers: Blocking Websites in Particular, IPR University Center 2015, p. 35.

[2] *Pihlajarinne, Taina*: Internet-välittäjä ja tekijänoikeuden loukkaus, Lakimiesliiton kustannus 2012, p. 140 and 149. Pihlajarinne also considers that filtering measures might constitute restrictions of freedom of expression as prohibited ex ante measures (at p. 51).

The interim injunctions can also be issued before the legal action is taken if the above-mentioned conditions are met, and provided that the rights of the author would otherwise be seriously jeopardized. Before the legal action is taken, a court may also order interim injunction without hearing the alleged infringer if this is deemed necessary due to the urgency of the case. Such an injunction will remain in force until further notice. After the injunction has been issued, the alleged infringer must be reserved an opportunity to be heard without delay. After hearing the alleged infringer, the court shall decide without delay whether it retains the injunction in force, or cancels it. Chapter 7 of the Judicial Procedure Code, which regulates precautionary measures, governs the legal safeguards for the measures to discontinue.

The new provision of Copyright Act, section 60 e, enables a court to order an intermediary (Internet Access Provider) to discontinue the making available of allegedly copyright infringing material when the claimed infringer is unknown. This is possible provided the making available of allegedly infringing material takes place to a significant extent without the consent of the author or it is obvious that the protection of the author's right would be otherwise seriously jeopardized. The claimant must provide information what actions it has taken in order to identify the alleged infringer. The order can be given on the condition that it is not considered unreasonable from the perspective of the alleged infringer, the intermediary, the recipient of the material and the author. The order may not jeopardize a third person's possibility to send and receive messages. The court treating the matter has to reserve the possibility for the intermediary to be heard before issuing the order. Such an order must be given for a fixed period of time, a maximum of one year at a time. It is possible to continue such an order for reasonable grounds. If the original reason ceases to exist, the court must cancel the order upon request by the concerned party. There is no case law yet applying section 60 e of the Copyright Act.

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.

Finland or Finnish courts haven't confronted any particular difficulties when considering remedies under the Consumer Sales and Guarantees Directive. Finnish approaches to remedies under the Consumer Sales and Guarantees Directive do not differ greatly from other Nordic countries.

Implementation of the Consumer Sales and Guarantees Directive did not cause any major changes when implemented with Government Proposal (89/2001) to the Finnish Consumer Act (38/1978), since the Act already con-

tained a similar level of consumer protection than was provided in the minimum harmonization directive. Amendments were mainly done to the Fifth Chapter of the Finnish Consumer Act. Those contained mainly amendments of technical nature, such as time limits (e.g. six month time period after lack of conformity becomes apparent.[3]

In some cases of a lack of conformity, pursuance of remedies might be relatively difficult for consumers. When the seller, the producer, or other intermediary is not willing to admit lack of conformity, consumer hasn't got that many options to seek remedies.

Consumers are entitled to bring free of charge their consumer claims before the Consumer Disputes Board in Finland as well as before a general court. Although the Consumer Disputes Board can only give unenforceable decisions, still businesses comply with its decisions in almost 80 % of cases.[4] However, access to general courts is not always *de facto* possible due to litigation cost risk. Due to lack of available of public information, it is hard to tell what challenges might the sellers been facing when pursuing remedies against producers or others in the chain of contracts, if any.

Question 1.2.2.

Maximum harmonisation has been widely criticised for lowering the Member States' existing standards of protection. Yet, both proposed Directives (*the Directive on certain aspects concerning contracts for the supply of digital content COM(2015)634 and the Directive on certain aspects concerning contracts for the online and other distance sales of goods COM(2015)635*) aim for full harmonisation. Full harmonisation implies that, after adoption of the directive, national laws may not exceed the terms of this legislation. Such a situation may not be welcomed by all Member States, especially if their national law proves to be originally stronger and more protective than the norms demanded by the Directive.

It does still seem that in order to guarantee a digital single market, where cross-border e-commerce can be conducted smoothly without additional expenses from the consumer as well as from the seller's side, full harmonisation is needed. Especially for all existing and emerging cross-border activities, full harmonisation is grounded. However, the harmonized norms should not lower existing standards of protection applicable in Member States.

[3] Consumer Sales and Guarantees Directive Art. 5(3).

[4] Consumer Disputes Board, Yearly Report, 2015. Accessible: http://www.kuluttajariita.fi/material/attachments/kuluttajariitalautakunta/kril/tujo/23G3ErbJ9/Toimintakertomus_2015.doc

Question 1.2.3.
The proposed Directive on certain aspects concerning contracts for the online and other distance sales of goods (COM(2015)635) fosters achievement of a genuine digital single market. However, achievement of genuine digital single market is hampered since services are excluded from the scope of the directive. Yet, certain problematic aspects relate to maximum harmonization nature of the proposed directive, since traditionally the level of consumer protection in the Nordic countries is relatively high in comparison to many other Member States.

Question 1.2.4.
If the Finnish consumer protection goes beyond the harmonisation suggested by the Commission in these two directives, it is to be questioned whether it would have a positive effect on the Finnish society. The main problem from the Finnish perspective is that the level of consumer protection is already high in Nordic states. Yet, it could be agreed that such harmonized rules could create legal certainty for businesses that operate intra-EU.

It should be also noted that consumer protection case law of the CJEU, by establishing the concept of "average consumer", differs relatively greatly from the Finnish court practice, i.e. upraising the concept of "passive consumer" who is not actively seeking for information.

Question 1.2.5.
Yes, although certain improvements could be done, especially with regard to the right to redress and enforcement. One option is to keep the harmonization at the same level. Yet, another option is to seek for more integration and provide for a mechanism to render enforceable consumer dispute -related awards or judgments.

Furthermore, as an essential "trigger" for further elements[5], it is not always clear whether an online platform provider qualifies as "trader" under the Unfair Commercial Practices Directive (2005/29/EC, UCPD) Art. 2(b). Yet, probably most of the online platforms qualify as a "trader", provided they charge a commission or provide additional services for a price.

Question 1.2.6.
Currently there hasn't been any known action before national courts against online providers' terms and conditions.

[5] E.g. Requirement to act with professional diligence (Art. 5(2) UCPD) and not to mislead consumer (Arts. 6(1)(f) and 7(1) UCPD).

Question 1.2.7.
In B2B context, in certain cases there exists a relatively significant difference of bargaining power between business entities and therefore the extension of B2C rules to B2B context could be justified. Yet, expanding the scope of the rules on B2C to B2B might involve problems, as the B2B contexts differ in many relevant respects from B2C contexts.

1.3. Geo-blocking

Question 1.3.1.
The condition "direct commercial activities to another Member State where the consumer has its domicile" of point (c) of Article 17(1) of Regulation (EU) 1215/2012 seems to be ideally aimed for e-commerce and like situations, in commercial contexts. Such "directing activities" require fixed business strategy (i.e. systematic and planned activities) of the trader to direct those activities to another Member States.

Article 1(5) of proposed Regulation COM(2016) provides legal clarity for businesses regarding the meaning of "directing activity". As called in the proposed regulation, just the mere fact that a trader is acting in compliance with the proposed regulation, it shall not be construed that trader is directing activities to another Member State where the consumer has its domicile. Hence, in certain cases, it is a necessity for businesses that courts from other Member States don't "automatically" obtain jurisdiction, particularly in those cases where a trader does not block access of consumers from another Member State to trader's online platform. Yet, more ambitious should motivate coordination towards unified approach of Brussels I regulation (1215/2012) and proposed regulation COM(2016).

1.4. Questions related to the collaborative economy

Question 1.4.1.
The state of law regarding collaborative economy is currently under various reforms. On the one hand, it is clear that collaborative economy businesses are protected by Section 18 of the Constitution which provides for right to conduct businesses. On the other hand, various parts of typical areas of collaborative economy are traditionally strictly regulated economies which have already had in impact to the existing forms of collaborative economy.

For instance, according to the analysis by the Ministry of Economic Affairs and Employment, the value of transactions in Finland's collaborative market was a little over EUR 100 million in 2016. The largest sectors were collaborative finance at 65%, accommodation and space at 19% and small tasks and household

services at 14%.[6] The relatively small share of collaborative traffic services can be estimated to be caused by the fact that traffic market has been strictly regulated in Finland. This is about to change when the Act on Transport Services enters fully into force in July 2018. The Act purports to promote the creation of new service models, ease market access, dismantle national regulation that limits competition and reduce the level of public guidance. In particular, the current system of limited number of taxi permits will be quashed. However, as result of delay of the reform, Uber has already decided to withdraw its primary service out of Finland until the new regulations allow a better business environment.

Question 1.4.2.
Yes, the consumer and competition authority in Finland has engaged actively in the discussions. As elsewhere, competition law liability concerning collaborative economy actors may be unclear. For example, providing an internet platform for the users might lead to competitively problematic scenarios (coordination of behaviour, even price fixing) as a combination of the platform and user actions, yet neither individual users, nor the platform provider might be liable for the emerging competition problems. Moreover, existing businesses and their joint organizations might seek to place restrictions on the introduction of new services, such as Uber or AirBnB. Existing businesses might also own essential facilities needed by the collaborative economy actors. So far, competition issues have predominantly emerged in the legislative processes, not in the form of enforcement decisions of the consumer and competition authority.

Question 1.4.3.
No definitive and concise answers can be given to these questions since the required authorizations and conditions for them depend on the area of business in questions. For instance, all kinds of access to transportation market requires specific licences whereas there are no similar hindrances. Hence, business strategy of Uber is not in line with current Finnish law whereas Airbnb is able conduct its businesses quite freely.

Question 1.4.5.
According to Section 5 of Chapter 1 of the Finnish Consumer Protection Act (38/1978) "*business* [trader] is defined as a natural person or a private or public legal person who, in order to obtain income or other economic benefit, deals in,

[6] See, Collaborative Economy in Finland –Current State and Outlook. Publications of the Ministry of Economic Affairs and Employment MEAE reports 9/2017. Available at http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79253/TEMrap_9_2017_verkkojulkaisu.pdf?sequence=1 (1 October 2017)

sells or otherwise offers consumer goods or services on a professional basis and for consideration." In essence, within the scope of consumer protection, to qualify as a trader, one needs to provide peer-to-peer services for pecuniary or other economic benefit. Yet, it should be noted that usually each Finnish act has own definitions for a "trader".

2. Digital media

Question 2.1.
Finnish national practice is in line with the judgment of 21 October 2015 in *New Media Online GmbH v Bundeskommunikationssenat* (case C-347/14), and yet, this case did not lead to different approach in Finland. However, there hasn't been yet any Finnish court practice regarding this issue.

Question 2.2.
Application of similar rules to operators that provide similar services could be supported. In current situation where AVMS rules are not applied to internet video platforms might be in the end of road, since it is most likely that boundaries between traditional service providers and video platforms will converge, at least into some extent.

Question 2.7.
Satellite and cable directive (93/83/EEC) is still relevant for Finland in cases of satellite and cable TV as well as radio broadcasting. Generally speaking, satellite and cable directive has operated relatively well in Finland and it has increased legal certainty. Yet, during the time of growing importance of IPTV services, it could be stressed that the Directive in its current form is losing its importance. However, it should be noted that currently regulation of on-demand video services is not that strict than e.g. regulation of linear television broadcasting.

Question 3.1.
Before the adoption of Regulation (EU) 2015/2120, Finnish Information Society Code contained more specific rules on net neutrality. Thus, such national rules were adopted on 1 January 2015. Those were replaced with rules on net neutrality of Regulation (EU) 2015/2120 in 2016. Government proposal of 67/2016 (to implement new rules on net neutrality) stressed the more consumer-favored approach taken by the Regulation (EU) 2015/2120. Yet, Regulation 2015/2120 provides additionally new supervision mechanism under Article 4, as well as more specific rules in general than Finnish national law on net neutrality was before.

Currently the Finnish Information Society Code (917/2014) regulates net neutrality in its Section 110. Section 110 makes direct reference to Regulation

(EU) 2015/2120 regarding rules of net neutrality. Yet, Finnish Communications Regulatory Authority may implement and give more specific executive order on technical characteristics of the internet access, inter alia. The Finnish Information Society Code does not take any stand towards zero-rating. Yet, the original net neutrality regulation gave a relatively wide discretion for Finnish Communication Regulatory Authority discretion to oblige operators and service providers to avoid practices and procedures, which have discriminatory function, or which could limit the "appropriate" use of internet communication.

Question 3.2.
Creation of a single market for telecommunications networks and/or services could be a feasible option and alternative e.g. to EU roaming related problems.

4. Data in the digital economy

Question 4.1.
Currently the work is still in progress. In 17.2.2016, Ministry of Justice appointed a Working Group "TATTI", to assess the legislative changes required by the national implementation of the General Data Protection Regulation (GDPR). The working group was also tasked to prepare a proposal for the national data protection law which would take into account the requirements stemming from GDPR. The work of the Working Group has been supported by two different research based reports on the "need to change national data protection statutes"[7] as well as on "business implications of GDPR"[8] from the IPR University Center, University of Helsinki, University of Lapland and University of Tampere. The research involved a preliminary assessment of approximately 800 statutes that contained nexus with data protection issues.

The Ministry of Justice appointed Working Group published its first report on 21 June 2017.[9] The report included a draft proposal for general data protection law. The general trend in the report is toward full harmonization. As a result, the margin of manoeuvre left for Member States by the GDPR has been used scarcely. In particular, the draft proposes that, excluding only provisions in the Article 56 and Chapter VII, the GDPR would be applicable in Finland also in such situations that would otherwise fall outside the scope of application pro-

[7] Olli Pitkänen (toim.): Tietosuojasäädösten muutostarve. Valtioneuvoston kanslia 2016. Available at http://tietokayttoon.fi/julkaisu?pubid=20302 (October 1 2016).
[8] Timo Enroth & Riku Neuvonen: EU:n tietosuoja-asetuksen yritysvaikutukset. Policy Brief 10/2017 http://tietokayttoon.fi/julkaisu?pubid=20401 (October 1, 2017)
[9] EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö. Ministry of Justice, 21 June 2016. The report is available at https://julkaisut.valtioneuvosto.fi/handle/10024/80098 (October 1, 2017).

vided by GDPR. Moreover, the possibility national derogations and more specific rules would only be used in a limited number of situations.

The Protection of employees' personal data is one such area. According to the working group report, the Act on the Protection of Privacy in Working Life – which is strict for employers in especially in fields such as electronic communications, should continue to stay in force without amendments. Thus, all companies in Finland are required to comply with the detailed national law in addition to the GDPR in respect of the personal data of employees.

In addition, there are areas of law that the working group The Working Group has not yet attained its final position. One of the key issues still remaining unresolved concerns the applicability of GDPR's administrative sanctions provisions to public authorities and bodies. However, majority of the Working Group members was of the opinion that those sanctions should also apply to the public authorities. Moreover, the Working Group did not reach definitive decision on the age limit of a child's consent in relation to information society services.

As to the concrete proposals, the draft proposal for implementing legislation includes a set of institutional reforms. The Working Group proposes that a Data Protection Agency (tietosuojavirasto) would be established to replace the current Office of the Data Protection Ombudsman. The Data Protection Ombudsman would continue as the head of the Agency. With regard to sanctions, a new Sanctions Board (seuraamuslautakunta) would be set up with a jurisdiction to impose the administrative sanctions as specified by the GDPR.

Finally, the Working Group will continue its work until the end of its term on 16 February 2018 during which it is continuing the assessment on the needs to reform different kinds of sectoral data protection legislation.

Question 4.2.

The attitudes and activities of businesses were investigated in a Government funded survey.[10] According to the results of survey, businesses were generally understanding the requirements stemming from the GDPR but were simultaneously troubled by the unpredictability of the changing regulatory landscape. Within the larger companies (turnover over € 50 million), over 90 % of the respondents estimated that GDPR will have significant impact on their business activities. This was mainly due to the strictly regulated conditions of consent, increasing compliance expenditures, new administrative sanctions as well as the unpredictability of new legal regime for data protection. The survey did

[10] Timo Enroth & Riku Neuvonen: EU:n tietosuoja-asetuksen yritysvaikutukset. Policy Brief 10/2017 http://tietokayttoon.fi/julkaisu?pubid=20401 (October 1, 2017)

not provide information about the activities of the companies related to privacy impact assessments and privacy by design.

Question 4.3.
Most of the above issues are so-called "open questions" in Finland. This said, no specific legislative measures or regulatory opinions or decisions have been implement. Furthermore, there has been made some initiatives to implement new test area for automated vehicles, such as for unmanned ships.

Question 4.4.
Status of "right to be forgotten" in Finland seems to be in line with the European practice. There are at least few known cases where complaints have been made before the Data Protection Ombudsman and national courts in Finland.

In judgment KHO 2016:208, Finnish Supreme Administrative Court cited the CJEU on Google Spain judgment, and confirmed the scope of definition of "controller" to cover search engines as well[11].

Furthermore, in a recent case, an individual had complained to the Finnish Data Protection Ombudsman about the removal of url-links from Google to websites, which contained medical information (in addition to information about his or her previous criminal activities). In a judgment of 8.12.2016[12], Helsinki Administrative Court ordered Google to remove access to two url-links, when the search is made by a name of this individual. In its judgment, the Court weighted individual's right to privacy as more supreme than others right to access such information. Yet, Google Spain judgment has been criticized with good reason, because it could increase excessively duties of search engines to remove search results, based on "right to be forgotten".

[11] Para 32.
[12] Helsinki Administrative Court, 8.12.2016 16/1028/5

FRANCE

Liza Bellulo • Laurence Calandri
Céline Castets-Renard • Olivia Tambou

1. Marché Intérieur et commerce électronique: Internet et commerce électronique

1.1. Commerce électronique, responsabilité des intermédiaires de l'Internet

Questions 1.1.1. et 1.1.2.

La délimitation du champ matériel d'application de la notion de prestataire de services intermédiaires a fait l'objet d'une patiente réflexion qui est loin d'être achevée, en raison d'une évolution fondamentale des circonstances des faits et des nombreux contentieux européens et nationaux qui sont nés en raison des imprécisions, volontaires ou non de la directive 2000/31/CE sur le commerce électronique. Le 8 juin 2000, lors de son adoption, il paraissait clair que seuls les intermédiaires techniques étaient visés par les règles dérogatoires de responsabilité limitée, prévues aux articles 12 à 15, dès lors que leur activité présentait un «*caractère purement technique, automatique et passif*» (considérant 42), dans le souci de ne pas freiner le développement d'internet. Mais, depuis lors, l'émergence de plate-formes jouant un rôle de mise en relation, de sélection, de référencement hiérarchisation, de promotion ou de régie publicitaire de plus en plus actif tend à remettre en cause la pertinence du critère présidant à la définition de l'hébergeur au sens de la directive 2000/31 et aboutissant à conditionner l'accès à l'information. A défaut de catégorie intermédiaire entre les hébergeurs et les éditeurs de services, ou de critère simple à mettre en œuvre pour caractériser un rôle actif, les juridictions françaises avaient longtemps hésité dans la manière de qualifier

certaines fonctions d'hébergement ou non, en s'appuyant sur le partage entre, d'une part, l'activité de stockage, incluant la mise en ligne d'annonces, qualifiée d'hébergement[1], et, d'autre part les activités promotionnelles et publicitaires, «relevant du droit commun»[2], ou, plus tardivement, sur un critère d'exploitation commerciale des sites pour mieux l'écarter[3].

La Cour de justice a, *in fine*, posé les jalons des éléments d'identification d'une activité intermédiaire dans les arrêts *Google* rendus le 23 mars 2010[4] en se fondant sur le considérant 42 et en imposant des conditions de neutralité, technicité et passivité pour l'appliquer aux moteurs de recherche[5], puis sur renvoi de la High court britannique[6] a clarifié le droit applicable en mettant un exergue un critère de rôle actif de classement des contenus, de nature à conférer au site une connaissance ou un contrôle des données relatives à ces offres, lorsqu'il prête une assistance consistant notamment à optimiser la présentation des offres à la vente en ligne ou à promouvoir ces offres. Dans un autre arrêt[7], en matière de protection des marques, la Cour a invité la juridiction de renvoi à vérifier le rôle du prestataire de référencement dans la rédaction du message commercial, mais, surtout, dans «*l'établissement ou la sélection de mots-clés*». L'arrêt n'exclut pas, en outre, un réexamen à la lumière d'autres «*circonstances*», en particulier si les parties démontrent que «*l'ordre des résultats naturels*» ne découle pas «*de la pertinence des sites respectifs par rapport au mot de recherche introduit par l'internaute*» et si la marque n'apparaît pas dans les premiers rangs des résultats naturels. La mise en œuvre pratique de ces critères n'est toutefois pas évidente dès lors que les opérateurs concernés invoquent souvent le recours aux algorithmes pour se décharger de toute responsabilité et que les constatations nécessaires à l'application des critères dégagés par la CJUE supposent la mise en œuvre de pouvoirs d'instruction approfondis qui ne sont pas toujours proportionnés aux enjeux du litige.

Sur le fondement de la jurisprudence de la CJUE, les juridictions françaises ont par exemple donné la qualification d'hébergeurs aux services de contenus

[1] Cour d'appel de Paris, 6 décembre 2006, *Abdel/zadi S. et SA Dounia c/SAS iEurop* et *SARL Lycos France* (au sujet de propos odieux).

[2] TGI Paris, 13 juin 2009, *L'Oréal contre e-bay.*

[3] Cass. 1ère Civ. 14 janvier 2010, *S. A. Dargaud Lombard et société Lucky Comics c/ S. A. Tiscali Media*; CA Paris, 7 juin 2006, *Tiscali Media c/ Dargaud Lombard*.

[4] CJUE, Gde Ch., 23 mars 2010, Google France Google, Inc. c/ Louis Vuitton Malletier (C-236/08); Viaticum SA, Luteciel SARL (C-237/08); Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08).

[5] Les questions préjudicielles posées à la CJUE dans les affaires Google, l'ont été par la Cour de cassation, laquelle a suivi sans surprise la décision de la Cour de l'UE: Cass. Com. 12 juil. 2012, (3 arrêts) Société Google c/ A. Rau et autres.

[6] CJUE, 12 juillet 2011, *L'Oréal SA et autres contre eBay International AG et autres* , C-324/09.

[7] CJUE, 23 mars 2010, *Google France & Google Inc./Louis Vuitton Malletier,* C-236/08, C-237/08 et C-238/08.

vidéo postés par les internautes (de type *Youtube* ou *DailyMotion*)[8] et aux sites agrégateurs d'informations[9]. En revanche, la première chambre civile de la Cour de cassation[10] a exclu l'application du régime d'irresponsabilité des intermédiaires techniques à l'activité de référencement d'œuvres protégées par le droit d'auteur.

Au-delà de la qualification des prestataires intermédiaires dans leurs activités commerciales, la mise en œuvre de cette notion a également été délicate en ce qui concerne la *liberté d'expression*. Le juge constitutionnel français[11] a veillé à préserver, sur le terrain de la liberté d'expression, avec des résultats équivalents à ceux poursuivis par la directive[12], le champ nouveau qu'a ouvert le développement de l'internet. Une diffusion élargie impose néanmoins également de nouvelles responsabilités et une conciliation avec les exigences de l'ordre public, par exemple vis-à-vis de propos susceptibles d'être poursuivis pénalement lorsqu'ils sont constitutifs d'apologie de crimes de guerre ou crimes contre l'humanité ou de terrorisme, et ceux de la protection de la réputation d'autrui, ou de la vie privée, et des données personnelles. Cet objectif légitime de politique publique est même susceptible d'impliquer un droit à l'oubli, tel que dégagé par la Cour de justice de l'Union européenne[13] avant que le législateur européen ne prenne le relais dans le nouveau règlement sur les données personnelles[14]qui entrera en vigueur en 2018. Le Conseil d'Etat[15] a récemment interrogé de nouveau la Cour, dans sa

[8] Cass. Com. 12 juil. 2012, (3 arrêts) Société Google c/ A. Rau et autres.

[9] CA Paris (14ᵉch., sect. B), 21 nov. 2008, *Blooblox Net c/ Olivier M*.

[10] Civ. 1ère , 12 juillet 2012 Nº de pourvoi : 11-15165 et 11-15188, FS-P+B+I.

[11] Le Conseil constitutionnel a émis une réservation d'interprétation dès l'adoption de la loi nº 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique (LCEN) qui transpose la directive 2000/31/CE en exigeant que les intermédiaires techniques empêchent l'accès au contenu «manifestement» illicite, dans le souci d'éviter des suppressions intempestives et portant atteinte à la liberté d'expression (DC nº 2004-496 du 10 juin 2004).

[12] Le Conseil constitutionnel a porté une réserve d'interprétation neutralisante du régime de responsabilité en cascade résultant de l'article 93-3 de la loi du 29 juillet 1982 sur la communication audiovisuelle, selon lequel le créateur ou l'animateur d'un tel site de communication au public en ligne peut voir sa responsabilité pénale recherchée, en qualité de producteur, à raison du contenu de messages dont il n'est pas l'auteur et qui n'ont fait l'objet d'aucune fixation préalable, dont il ne peut s'exonérer des sanctions pénales qu'il encourt qu'en désignant l'auteur du message ou en démontrant que la responsabilité pénale du directeur de la publication est encourue au regard de l'exercice de la liberté d'expression et de communication protégée par l'article 11 de la Déclaration de 1789. Il a jugé que ces dispositions ne sauraient être interprétées comme permettant que cette personne voie sa responsabilité pénale engagée en qualité de producteur à raison du seul contenu d'un message dont il n'avait pas connaissance avant la mise en ligne (CC, Décision nº 2011-164 QPC du 16 septembre 2011, *M. Antoine J*)

[13] CJUE, 13 mai 2014, *Google Spain SL, Google Inc. contre Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez*, C-131/12.

[14] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[15] CE, 24 février 2017, *Mme C, M. F, M. H, M. D*, nos 391000, 393769, 399999, 401258.

formation contentieuse la plus solennelle, sur la portée concrète de ce droit, en particulier à l'égard d'un moteur de recherche: peut-il et doit-il être qualifié de responsable de traitement? A défaut quelles exigences lui sont-elles applicables? Est-il tenu de faire systématiquement droit aux demandes de déréférencement portant sur des liens menant vers des pages web qui traitent de telles données? Peut-il appliquer de lui-même les exceptions prévues par la directive 95/46/CE sur la protection des données personnelles? Une page internet, comportant des données faisant état des condamnations ou des procédures judiciaires dont une personne physique a été l'objet, doit-elle être systématiquement déréférencée? Quelle est la portée géographique du droit au déréférencement fondé sur la directive 95/46/CE?[16] L'exercice de ce droit permet-il d'imposer un déréférencement sur un moteur de recherche identifié en «.com» d'audience mondiale?

Ces difficultés de délimitation de la notion de prestataires de services intermédiaires et, par conséquent, d'exonération de la responsabilité qui y est attachée ont suscité un débat sur l'opportunité de faire évoluer ces règles tout en préservant le potentiel de croissance et de liberté d'expression de l'internet. Dans l'attente de propositions de portée européenne que le Conseil d'Etat avait déjà appelée de ses vœux en 2014 dans son étude annuelle sur le Numérique et les droits fondamentaux et de la mise en œuvre concrète de la feuille de route dressée par la Commission européenne en mai 2016, confirmée en mai 2017[17], le législateur français est intervenu, par la loi nº 2016-1321 du 7 octobre 2016 pour une République Numérique pour définir les *«plateformes»*[18] et esquisser des obligations d'information loyale, claire et transparente notamment sur les conditions générales d'utilisation, les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels elles permettent d'accéder, l'existence d'une relation contractuelle, d'un lien capitalistique ou d'une rémunération à leur profit, dès lors qu'ils influencent le classement ou le référencement des contenus, des biens ou des services proposés ou mis en ligne.

Revenant de façon plus spécifique sur l'économie collaborative, l'étude annuelle du Conseil d'Etat de 2017, «*Puissance publique et plateformes numériques:*

[16] Le Conseil d'Etat a posé une question préjudicielle sur ce point à la CJUE: Conseil d'Etat, Sect. du contentieux, 10e – 9e ch. Réunies, décision du 19 juillet 2017.

[17] COM(2016) 288 final et COM(2017) 228 final.

[18] L'article 49 de la loi, désormais codifié à l'article L. 111-7 du code de la consommation, qualifie d'opérateur de plateforme en ligne «toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur: 1º Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers; 2º Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service».

accompagner l'ubérisation»[19], suggère un ensemble équilibré de mesures complémentaires au niveau européen, mais aussi national: d'une part, à la charge des plateformes, l'institution de règles plus larges de loyauté et de responsabilité dans l'utilisation des algorithmes, incluant des mécanismes d'arrêt d'urgence, ainsi que des règles assurant l'équité fiscale et sociale entre l'économie traditionnelle et l'économie numérique, d'autre part, la promotion d'un environnement favorable à l'essor des plateformes, par le soutien à l'entreprenariat individuel, la simplification administrative au profit de leurs collaborateurs, et des études d'impact systématiques de nouvelles réglementations en ce qui concerne leurs effets sur l'économie «agile». La Commission européenne a d'ores-et-déjà proposé le 21 septembre 2017, dans sa communication des options de court terme en matière d'équité fiscale[20] et annoncé des actions ciblées sur les clauses contractuelles et pratiques commerciales déloyales constatées dans les relations de plateforme à entreprise. Le renforcement du réseau européen de la concurrence, prévu par une proposition de directive en cours d'examen, reste également indispensable, mais sans doute insuffisant à lui seul pour leur permettre de réagir plus rapidement à des risques d'abus d'éviction potentiellement durables, notamment par l'usage des mesures conservatoires. La récente décision de la Commission européenne sanctionnant Google par une amende de 2,42 milliards d'euros et prononçant une injonction à son égard[21] a ainsi nécessité une enquête de plus de sept ans.

Question 1.1.4.

Le régime de responsabilité limitée des hébergeurs ne fait pas obstacle, en lui-même, au prononcé d'injonctions de retrait de contenus manifestement illicites, qui peuvent être adressées à tout intermédiaire, comme l'a confirmé la Cour de justice[22], et dont l'inexécution est susceptible d'engager leur responsabilité, conformément au considérant 46 de la directive 2000/31[23].

En ce qui concerne les injonctions motivées par des *considérations d'ordre public*, ce sont, compte tenu de la compétence des Etats membres, en l'absence de mesure d'harmonisation, des dispositifs nationaux qui en ont dessiné les contours. Ainsi,

[19] http://www.ladocumentationfrancaise.fr/rapports-publics/174000714-etude-annuelle-2017-du-conseil-d-etat-puissance-publique-et-plateformes-numeriques

[20] COM(2017) 547 final, «A fair and efficient Tax System in the European Union for the Digital Single Market».

[21] *Commission européenne, 27 juin 2017, COMP.39740, Google Search (Shopping).*

[22] CJUE, 27 mars 2014, *UPC Telekabel Wien GmbH*, C-314/12.

[23] Il précise à cet effet expressément que l'hébergeur «doit, dès qu'il prend effectivement connaissance ou conscience du caractère illicite des activités, agir promptement pour retirer les informations concernées ou rendre l'accès à celles-ci impossible. Il y a lieu de procéder à leur retrait ou de rendre leur accès impossible dans le respect du principe de la liberté d'expression et des procédures établies à cet effet au niveau national».

en France, l'article 12 de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a prévu que «*lorsque les nécessités de la lutte contre la provocation à des actes terroristes ou l'apologie de tels actes relevant de l'article 421-2-5 du code pénal ou contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du même code le justifient, l'autorité administrative*» «*peut demander*» indifféremment à l'éditeur ou à l'hébergeur «*le retrait des contenus*» qui contreviennent à ces mêmes articles, dans le cadre de l'exercice de ses pouvoirs de police administrative. La légalité des décrets pris l'application de cette disposition[24], qui avait été contestée devant le Conseil d'Etat, a été confirmée, au motif, notamment que les dispositifs de blocage et de déréférencement «*ont pour objectifs légitimes, d'une part, de restreindre, pour les internautes de bonne foi, l'accès aux sites provoquant à des actes de terrorisme ou en faisant l'apologie et aux sites diffusant des images et représentations de mineurs à caractère pornographique et, d'autre part, de gêner l'accès volontaire de certains internautes à ces contenus*», qu'il ne résulte pas des stipulations de l'article 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales que de telles mesures ne puissent être ordonnées que par un juge, et que la loi prévoit des garanties appropriées, notamment la transmission de la liste des adresses électroniques à bloquer ou à déréférencer à une personnalité qualifiée, désignée en son sein par la Commission nationale de l'informatique et des libertés qui peut s'assurer de la régularité des demandes, ainsi que l'obligation à la charge de l'autorité administrative de mettre à jour trimestriellement les adresses électroniques qui lui sont notifiées[25].

En ce qui concerne les injonctions *au titre de la lutte contre la contrefaçon ou le piratage, qui* permettent ainsi de protéger des droits de propriété intellectuelle sans lesquels aucune production de contenus susceptible d'être diffusée sur internet ne saurait se développer, le droit dérivé a défini certaines caractéristiques communes[26]. Néanmoins, ces dispositions laissent une large marge d'appréciation aux juges et donnent lieu à des pratiques très diverses. La CJUE a jugé que le prononcé de telles injonctions ne pouvait aboutir à imposer aux hébergeurs une obligation de surveillance permanente et généralisée des informations hébergées placées sur leur site, qui porterait une atteinte disproportionnée à la liberté

[24] Décret nº 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique et décret nº 2015-253 du 4 mars 2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.

[25] CE, 15 février 2016, *Association French data network et autres*, nºs 389140, 389896, 2ème et 7ème s-s.

[26] article 11 de la Directive 2004/48/CE du 29 avril 2004 relative au respect des droits de propriété intellectuelle et son considérant 23; considérant 59 de la Directive 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information

d'entreprendre des prestataires techniques et à la liberté de communication[27]. La Cour de cassation a reçu cette jurisprudence par un arrêt du 12 juillet 2012 dans lequel elle a jugé que les injonctions devaient être limitées à «*la seule faculté d'ordonner une mesure propre à prévenir ou à faire cesser le dommage lié au contenu actuel du site en cause*» à l'exclusion de toute mesure de surveillance et de filtrage des contenus illicites futurs et de tout dispositif de blocage illimité[28].

Question 1.1.3.

La mesure dans laquelle des obligations de précaution ou de diligence peuvent être imposées reste encore à déterminer, en ce qui concerne, d'une part, les injonctions de retrait dites prolongées, et, d'autre part, le devoir de précaution des intermédiaires.

Dans l'affaire dite Allostreaming[29], le tribunal de grande instance de Paris a ainsi ordonné, des mesures de blocage[30] pour une durée de douze mois, mais n'a pas fait droit à la demande des associations de les autoriser à utiliser un outil qu'ils avaient conçu[31] permettant la mise à jour des injonctions du tribunal[32]. La difficulté tenait au fait qu'en présence de la réapparition des contenus retirés, il ne s'agit pas de suivre l'exécution de la décision de blocage mais de permettre au juge d'étendre les effets de sa première décision en présence d'une nouvelle atteinte aux droits d'auteur (ex: création d'un nouveau site ou duplication de son contenu dans un autre site existant ou créé). Or, en matière de procédure civile, le juge est dessaisi dès qu'il rend sa décision; lui confier dès lors le soin de veiller aux possibles contournements de sa décision modifie nettement son office. De même, dans trois arrêts concernant la société *Google*, la Cour de cassation a censuré une obligation d'empêcher le repost (*notice and stay down*)[33].

[27] CJUE, 24 novembre 2011, *Scarlet Extended*, C-70/10 et *SABAM*, C-360/10.

[28] Cass. Civ. 1, 12 juillet 2012, *André Rau c/ Google & Au Féminin.com*, nº 11-15.167 et nº11-15.188.

[29] TGI Paris, réf., 28 novembre 2013, *Association des Producteurs de Cinéma (APC), la Fédération Nationale des Editeurs de Films (FNDF) et le Syndicat de l'Edition Vidéo Numérique (SEVN*), RG nº 11/60013. Voir aussi jugements du TGI de Paris du 22 octobre 2015 (Pirate Bay), 4 décembre 2014, 2 avril 2015, 2 juillet 2015.

[30] tendant à interdire l'accès à plusieurs sites internet qui mettaient exclusivement à disposition des internautes des liens non autorisés permettant de visionner des œuvres protégées en streaming ou de les télécharger, par tout moyen efficace et notamment par le blocage des noms de domaine, à l'encontre des principaux fournisseurs d'accès internet, et leur référencement par les moteurs de recherche.

[31] Logiciel développé par TMG (Trident Media Guard, prestataire d'ores et déjà utilisé en matière de peer-to-peer pour transmission à l'HADOPI) qui notamment détecte les modifications de noms de domaines, les changements d'adresses IP,alerte les moteurs de recherche et les FAI, pour obtenir leur déréférencement ou leur blocage sans nouvelle saisine du juge.

[32] En pratique, aux termes de l'assignation, un agent assermenté de l'ALPA aurait été autorisé par avance par le juge à notifier aux FAI, soit des levées de blocage, soit l'extension des blocages d'origine à de nouveaux noms de domaine et/ou adresses IP.

[33] Cass. 1ère Civ., 12 juil. 2012 (3 arrêts concernant Google), nº 11.15-165, nº 11.15-188, nº 11-13.666, nº 11-13.669.

Dans ce contexte, diverses réflexions ont été conduites en France afin de tenter de remédier à ces difficultés, notamment dans le rapport «*Outils opérationnels de prévention et de lutte contre la contrefaçon en ligne*» de mai 2014, de Mireille Imbert Quaretta et Louis Dutheillet de Lamothe[34] et l'étude annuelle «*Numérique et droits fondamentaux*» du Conseil d'Etat en 2014[35], qui propose de créer au niveau européen un tiers statut entre ceux d'hébergeurs et d'éditeurs pour les plateformes, mettant à leur charge certaines obligations de loyauté (voir également la section 1.4). Ces études ont également nourri le développement de codes de bonne conduite qui prévoient des mesures équilibrées entre les titulaires de droits et certains acteurs de l'internet: une charte des bonnes pratiques de la publicité en ligne[36], une coopération spécifique avec les plates-formes de commerce en ligne[37], les sites de petites annonces entre particuliers[38], et les opérateurs postaux[39] prévoyant notamment la mise en place par les plates-formes de mécanismes d'analyse du contenu des offres et du comportement des vendeurs et des notifications portant sur des offres de contrefaçon par les titulaires de droits aux plates-formes. Des réflexions sont en cours en vue de l'élargissement de ces actions à l'ensemble des droits de propriété intellectuelle[40].

[34] http://www.culturecommunication.gouv.fr/Documentation/Rapports/Outils-operationnels-de-prevention-et-de-lutte-contre-la-contrefacon-en-ligne

[35] http://www.conseil-etat.fr/Decisions-Avis-Publications/Etudes-Publications/Rapports-Etudes/Etude-annuelle-2014-Le-numerique-et-les-droits-fondamentaux

[36] http://www.culturecommunication.gouv.fr/Actualites/Charte-des-bonnes-pratiques-dans-la-publicite-pour-le-respect-du-droit-d-auteur-et-des-droits-voisins

[37] Charte de lutte contre la contrefaçon sur Internet entre titulaires de droits de propriété industrielle et plateformes de commerce électronique, ouverte à la signature le 16 décembre 2009.

[38] Charte de lutte contre la contrefaçon sur Internet entre titulaires de droits de propriété industrielle et plateformes de petites annonces sur Internet, ouverte à la signature le 7 février 2012.

[39] Charte de lutte contre la contrefaçon sur Internet entre titulaires de droits de propriété industrielle et opérateurs postaux, ouverte à la signature le 7 février 2012.

[40] En matière de coopération avec les acteurs de la publicité sur internet, le CNAC a pour objectif de :
– élaborer une charte des bonnes pratiques dans la publicité sur internet pour le respect des droits de propriété intellectuelle engageant les acteurs de la publicité sur internet et les représentants des titulaires de droits,
– créer un comité de suivi des bonnes pratiques dans la publicité sur internet pour le respect des droits de propriété intellectuelle.
En matière de coopération avec les opérateurs du paiement en ligne, le CNAC étudie la possibilité de:
– créer un comité de suivi des bonnes pratiques dans les moyens de paiement en ligne pour le respect des droits de propriété intellectuelle ;
– mettre en place un guichet unique chargé de centraliser le traitement des plaintes des consommateurs et des titulaires de droits, et de faciliter l'accès des entreprises, en particulier des PME, à un blocage des comptes bancaires des contrefacteurs effectué par les opérateurs de paiement à distance. Ce dispositif repose sur le mécanisme de rétro-facturation («chargeback»), repris dans la politique commerciale des opérateurs de paiement à distance. Il est déjà mis en œuvre aux Etats-Unis (International Anti-Counterfeiting Coalition) et au Canada (Centre Anti-Fraude).

Le législateur s'est, sans attendre l'aboutissement de ces réflexions de portée générale qui ont en particulier été suscitée par le piratage d'œuvres musicales ou audiovisuelles, intéressé au référencement des œuvres d'art plastiques, graphiques ou photographiques. L'article 30 de la loi nº 2016-925 du 7 juillet 2016 relative à la liberté de création, à l'architecture et au patrimoine. L'article 30 concerne la recherche et le référencement, codifié à l'article L. 136-1 du code de la propriété intellectuelle, définit ce service[41], sans considération quant au caractère licite ou non de la mise en ligne originelle, et institue leur gestion collective automatique par des sociétés agréées, qui sont seules habilitées à conclure les conventions avec leurs exploitants aux fins d'autoriser la reproduction et la représentation des œuvres d'art plastiques, graphiques ou photographiques, selon un modèle inspiré des sociétés de gestion collective des droits d'auteur. Dans cette hypothèse, l'activité de référencement n'est pas une simple activité d'hébergement dans la mesure où est reconnue une utilisation des œuvres (reproduction et représentation), impliquant le versement d'une redevance obligatoire à une société de gestion collective. On attend alors une coopération bien plus forte du référenceur qui doit rémunérer le contenu financé, sauf à le retirer. Cependant, la mise en œuvre concrète de cette mesure s'avère complexe et des contentieux ont été engagés pour la contester.

Au niveau européen, la conformité des injonctions de retrait (procédure dite «*notice and keep off*» ou «*notice, take down & stay down*») prolongé, pratiquées aux Etats-Unis, au Royaume-Uni, en Italie et en Espagne, visant à assurer l'absence de réapparition d'un contenu bloqué ou supprimé, n'est ainsi pas encore solidement affirmée, notamment au regard de la liberté de communication, même si la Cour a donné des indications positives en ce sens dans l'arrêt *Telekabel* précité[42]. Si le principe des injonctions ainsi définies a été confirmé, la Cour d'appel de Paris a cependant jugé[43] que les frais ne pouvaient être assumés par les hébergeurs, dans le prolongement d'une décision en ce sens du Conseil constitutionnel[44].

[41] *«On entend par service automatisé de référencement d'images, au sens du présent chapitre, tout service de communication au public en ligne dans le cadre duquel sont reproduites et mises à la disposition du public, à des fins d'indexation et de référencement, des œuvres d'art plastiques, graphiques ou photographiques collectées de manière automatisée à partir de services de communication au public en ligne».*

[42] CJUE, 12 juillet 2011, *L'Oréal SA et autres contre eBay International AG et autres*, C-324/09. en soulignant que l'injonction devait «laisser à son destinataire le soin de déterminer les mesures concrètes à prendre pour atteindre le résultat visé de sorte que celui-ci peut choisir de mettre en place des mesures qui soient les mieux adaptées aux ressources et aux capacités dont il dispose et qui soient compatibles avec les autres obligations et défis auxquels il doit faire face dans l'exercice de son activité», lui permettre «de s'exonérer de sa responsabilité en prouvant qu'il a pris toutes les mesures raisonnables» et a estimé que les injonctions devaient également pouvoir permettre de prévenir de nouvelles atteintes.

[43] CA Paris, 15 mars 2016, *Association des producteurs de cinéma et autres*, nº 040/2016.

[44] Conseil constitutionnel, 28 décembre 2000, Décision 2000-441 DC.

Au-delà des injonctions, il convient également de fixer la nature de l'obligation de précaution/diligence à la charge des intermédiaires poursuivant une finalité commerciale, que ce soit par la révision de la directive 2001/29/CE sur le droit d'auteur ou la jurisprudence.

La proposition de directive sur le droit d'auteur dans le marché unique numérique (COM(2016) 593 final) a prévu en son article 13 et son considérant 39 des dispositions relatives à l'utilisation de contenus protégés par des prestataires de services de la société de l'information qui stockent et donnent accès à un grand nombre d'œuvres et d'autres objets protégés chargés par leurs utilisateurs: dispositifs de reconnaissance et marquage des œuvres proportionnés aux moyens des plateformes, dispositifs de traitement des plaintes liées à l'application de ces mesures, coopération avec les titulaires de droits pour faire évoluer les mesures techniques.

Concomitamment à cette proposition, deux arrêts de la Cour de justice ont précisé la notion de «communication au public» prévue à l'article 3 de la directive 2001/29, qui constitue l'assiette de la rémunération des auteurs, et n'avait pas été modifié par la proposition. Leur impact, potentiellement majeur, reste à déterminer. En septembre 2016, la Cour a ainsi jugé[45] que le placement à but lucratif de liens hypertexte donnant accès à des œuvres protégées profonds à but lucratif devait être constitué comme communiquant au public cette œuvre, et que la personne qui place le lien était tenue de vérifier que l'offre était licite. Cette présomption est réfragable, mais la cour ne précise pas par quel moyen (démonstration de la prise de diligences raisonnables? comment celles-ci peuvent être appréciées?), ni quelles sont les personnes qui entrent dans le champ de cette présomption. En revanche, une telle présomption n'est pas mise en œuvre pour les liens à but non lucratif, compte tenu de la primauté de la liberté d'expression. Pour bénéficier de cette présomption, les titulaires de droit doivent néanmoins montrer qu'un public nouveau a été touché du fait de ces hyper-liens. Or, par deux autres arrêts de 2017[46], relatif à des services de pair à pair il semble que la cour ait fortement nuancé l'application de sa jurisprudence antérieure qui concevait cette notion de manière restrictive[47]; la Cour semble désormais considérer que des internautes accédant à des œuvres piratées, même si celles-ci avaient déjà été publiées sur internet, pouvaient constituer un «*public qui n'a pas été pris en compte par les titulaires du droit d'auteur lorsque ces derniers ont autorisé la communication initiale*». Cette interprétation demeure toutefois à confirmer compte tenu des nombreuses nuances que la jurisprudence comporte au cas par cas, comme l'a

[45] CJUE, 21 septembre 2016, *GS Media*, C-160/15.

[46] CJUE, 26 avril 2017, *Stichting Brein*, C-527/15; 17 juin 2016, *Stichting Brein*, C-610/15.

[47] CJUE, 13 février 2014, *Svensson*, aff. C-466/12 (à propos d'hyper-liens); ord. 21 octobre 2014, *Bestwater*, C-348/13 (à propos d'insertions).

relevé un récent rapport du professeur Sirinelli[48] et de l'absence à ce jour d'arrêt solennellement rendu en grande chambre.

1.2. Protection des consommateurs en matière d'Internet et de commerce électronique, d'achats sur internet et de droits contractuels; protection des consommateurs et résolution de litiges [49]

Questions 1.2.2. et 1.2.3.

Sous réserve des particularités liées au droit d'auteur et aux droits voisins attachés à ces contenus numériques et de la nécessité de règles technologiquement neutres vis-à-vis de la diversité des modalités de mise à disposition, les contrats de vente portant sur des contenus numériques relèvent indéniablement des rapports de consommation. A titre d'exemple, si l'on prend le cas d'un fichier musical, le contrat serait qualifié de vente s'il est gravé sur un CD mais le serait différemment s'il était téléchargé. Pour autant, pour le consommateur, l'aboutissement et l'intérêt sont les mêmes, à savoir écouter l'œuvre musicale. La lisibilité, l'accessibilité et la cohérence du droit applicable sont l'un des premiers facteurs de confiance du consommateur dans le marché intérieur. Aussi, l'élaboration d'un corps de règles rassemblant les dispositions applicables à l'ensemble des biens doit être privilégiée (comme c'est le cas dans la directive 2011/83/CE relative aux droits des consommateurs, qui couvre les contrats de vente de biens matériels et les contenus numériques fournis sur un support matériel ou non en adaptant, pour ces derniers, les règles applicables).

Toutefois, il convient de prendre en compte la spécificité, pour ce type de contrats, de l'approche relative à la hiérarchie des remèdes à l'inexécution contractuelle entre l'exécution en nature (remplacement ou réparation du bien),

[48] http://www.culturecommunication.gouv.fr/Politiques-ministerielles/Propriete-litteraire-et-artistique/Conseil-superieur-de-la-propriete-litteraire-et-artistique/Travaux/Missions/Mission-du-CSPLA-sur-le-droit-de-communication-au-public

[49] Document de travail des services de la Commission [SWD](2016)163 Orientations concernant la DPCD [Directive relative aux pratiques commerciales deloyales]. Dans le cadre d'une évaluation au cas par cas, un prestataire de plate-forme peut agir à des fins qui entrent dans le cadre de son activité commerciale dès lors, par exemple, qu'il facture une commission sur les transactions entre fournisseurs et utilisateurs, fournit des services supplémentaires payants ou tire des recettes de publicités ciblées. En outre, au titre de l'article 5, paragraphe 2, de la DPCD, aucun prestataire de plate-forme ayant qualité de «professionnel» ne devrait contrevenir aux exigences de la diligence professionnelle dans ses pratiques commerciales vis-à-vis du consommateur. Au titre de l'article 2, point h), de la DPCD, on entend par "diligence professionnelle" le niveau de compétence spécialisée et de soins dont le professionnel est raisonnablement censé faire preuve vis-à-vis du consommateur, conformément aux pratiques de marchés honnêtes et/ou au principe général de la bonne foi dans son domaine d'activité. Les obligations de diligence professionnelle vis-à-vis des consommateurs imposées à ces professionnels par la DPCD se distinguent, tout en le complétant, du régime d'exemption de responsabilité établi par l'article 14 de la directive sur le commerce électronique pour les informations illicites hébergées par des prestataires de service à la demande de tierces parties.

la réduction du prix, la résolution du contrat ou une indemnisation. L'ensemble de ces sanctions ne paraissent pas applicables à l'ensemble des contenus numériques. Tel est par exemple le cas du remplacement ou de la réparation, assimilés à une exécution en nature, qui parait difficilement compatible avec les contenus relevant de la législation relative aux droits d'auteur. Le choix offert au consommateur entre ces différents remèdes doit donc être encadré afin d'éviter les abus si le coût de la solution choisie par le consommateur est disproportionné au regard de la valeur du bien ou de l'importance du défaut de conformité. D'autre part, ces propositions ne doivent pas se traduire par un affaiblissement du niveau de protection actuellement offert, en particulier en matière de clauses abusives.

Question 1.2.5.
La directive 2011/83/UE du 25 octobre 2011 relative aux droits des consommateurs venant à peine d'être transposée dans les législations nationales des États membres, il est difficile d'en mesurer aujourd'hui les effets sur le marché intérieur. Si cette législation est globalement adaptée, le cadre européen pourrait davantage assurer la loyauté de l'information (information sur l'existence de relations contractuelles ou de liens capitalistiques avec les personnes référencées), introduire des obligations relatives à la fiabilité et l'intégrité des avis des utilisateurs, garantir la portabilité des données de consommation et des contenus légalement acquis, pour des raisons tant de protection des consommateurs, que de développement d'une concurrence «en silos» entre plateformes intégrées.

Question 1.2.6.
Devant les juridictions françaises, peut être citée l'affaire dite «L'origine du monde», opposant Facebook à l'un de ses utilisateurs, par laquelle le réseau social a supprimé l'accès à la reproduction de l'œuvre de Gustave Courbet. Dans un arrêt du 12 février 2016, la Cour d'appel de Paris[50] s'est reconnue compétence en application des articles 15 et 16 du règlement 44/2001 pour statuer sur la licéité de la clause attributive de compétence issue des conditions générales d'utilisation (CGU) de *Facebook*, bien que rédigée au profit des tribunaux d'Etat et fédéraux situés dans le comté de Santa Clara, en Californie, et jugé que cette clause, rédigée au détriment du consommateur et créant un déséquilibre significatif devait être regardée comme abusive et, dès lors, réputée non écrite.

Question 1.2.7.
Il semble qu'il faille être prudent dans l'extension des règles concernant les relations entre entreprises et consommateurs (B2C) aux relations entre entreprises (B2B). L'urgence et surtout la pertinence d'une telle solution restent à démontrer.

[50] Cour d'appel de Paris, Pôle 2 – Chambre 2, arrêt du 12 février 2016, Facebook Inc. / Monsieur X.

1.4. Questions liées à l'économie collaborative

Question 1.4.1.

Parmi les questions les plus controversées concernant les entreprises de l'économie collaborative, on peut citer l'activité des plateformes de mise en relation entre les VTC et les consommateurs, clients de la plateforme de type Uber.

La combinaison de l'obligation de notification préalable qui découle de la directive nº 2015/1535/UE prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information et du principe du pays d'origine fixé par l'article 3 de la directive sur le commerce électronique, qui fixe de fait une règle de conflit de lois de droit public en matière de réglementation des plate-formes et les exonère largement de leur responsabilité (voir 1.1.) explique sans doute que les contentieux en matière d'autorisations administratives requises des acteurs de l'économie collaborative se soient à ce jour relativement peu développés sur le fondement du droit de l'Union européenne, hormis le cas particulier du service de transport de particuliers fourni par Uber.

Mais c'est sans doute essentiellement parce que le secteur des transports échappe au champ de la directive 2000/31 ainsi qu'à celui, plus généralement, de la liberté de prestation de services. En effet, les services de transport relèvent de l'article 58 TFUE et échappent en conséquence, en l'absence de mesure d'harmonisation prise sur le fondement de l'article 91, paragraphe 1 TFUE, à la liberté de prestation de service prévue par l'article 56 TFUE et au principe du pays d'origine tiré de la directive 2000/31. C'est le cas plus particulièrement des activités de transport individuel de personnes à titre onéreux ou gratuit de moins de dix places, qui ne font l'objet d'aucune disposition de droit dérivé. Le dialogue des juges joue alors pleinement, une série de questions préjudicielles étant en cours d'examen. Les conclusions récemment rendues dans l'affaire C-434/15, si elles étaient confirmées, semblent permettre de retenir la qualification de service de transport dans la mesure où un faisceau d'indices tend à conférer à la plate-forme un rôle essentiel dans la définition du service: la finalité de la mise en relation d'une part, et le rôle que joue la plate-forme d'autre part pour définir le lieu de prise en charge du client, gérer les moyens informatiques, fixer des conditions qualitatives d'exécution du service, qu'il s'agisse du véhicule, ou du chauffeur (critères de sélection de l'appartenance au réseau et d'exclusion du réseau, notamment selon l'appréciation du client de la prestation fournie), et, surtout, le prix. Les mêmes critères semblent devoir être retenus pour déterminer la portée de l'obligation de notification préalable au titre de la directive 2015/1535 au regard des conclusions prononcées dans l'affaire C-320/16, sur renvoi du tribunal de grande instance de Lille.

Toutefois, d'autres questions resteront encore à explorer par les juges dans le domaine de l'économie collaborative, notamment l'importance de certains

critères proposés dans la communication de la Commission sur l'économie collaborative du 2 juin 2016[51], tels que la propriété du véhicule ou le risque assumé par le conducteur[52].

Question 1.4.2.

La règle de conflit de lois en matière de réglementation prévue par la directive commerce électronique n'est pas aussi contraignante pour les autorités administratives indépendantes nationales chargées de la régulation lorsqu'elles s'appuient sur des règles harmonisées au niveau européen. Ces règles peuvent résulter directement du droit primaire, comme c'est le cas pour les pratiques anti-concurrentielles, ou de règles de droit dérivé spéciales, comme c'est le cas notamment en matière de protection des données personnelles. Ces autorités disposent en outre de certains pouvoirs (auto-saisine, instruction, injonction, souscription d'engagements, sanctions pécuniaires) plus adaptés à une action efficace et transnationale au niveau européen. C'est donc essentiellement sur ce terrain que les principales questions juridiques relatives à l'économie collaborative se sont développées, ou du moins de la façon la plus visible.

L'Autorité de la concurrence française a été l'une des premières en Europe à analyser le fonctionnement des marchés de la publicité en ligne sur lesquels l'acteur dominant a été mis face à ses responsabilités, dès 2010[53]. Elle a estimé dans un avis que Google, pour la publicité liée aux recherches, et Pages jaunes, pour la publicité sur les annuaires en ligne, disposaient, sur leur marchés respectifs, d'une position dominante compte tenu d'un faisceau d'indices convergents, et pointé en conséquence les responsabilités particulières qui leur incombaient[54],

[51] http://ec.europa.eu/DocsRoom/documents/16881

[52] Si ces facteurs ne semblent pas pertinents pour déterminer la portée de l'article 58 TFUE, puisqu'ils sont étrangers à la relation entre la plate-forme et le client et le consentement de ce dernier à souscrire un service (lieu de prise en charge, temps d'attente, prix, partage ou non du véhicule avec d'autres clients), ils peuvent être essentiels pour apprécier les relations entre la plate-forme et ses contributeurs au regard du droit de la concurrence, au titre de l'article 101 TFUE, et par conséquent pour déterminer la portée de l'interdiction de l'imposition des prix de détail, qui ne résultent pas seulement du taux de commission perçu par la plate-forme, ou pour apprécier les éventuelles restrictions apportées à la concurrence inter-plate-formes que peuvent faire jouer les contributeurs. Il reste par ailleurs curieux que certaines plate-formes puissent à la fois estimer qu'elles sont exonérées du respect des législations sur le travail salarié compte tenu de l'autonomie de leurs contributeurs, qui ne répondent pas dès lors au critère essentiel de subordination, mais qu'elles le sont également des règles de concurrence applicables aux restrictions verticales.

[53] Avis 10-A-29 du 14 décembre 2010 sur le fonctionnement concurrentiel de la publicité en ligne.

[54] Afin que le jeu concurrentiel puisse s'exercer pleinement, les acteurs en position dominante doivent s'abstenir de mettre en œuvre deux types de pratique conduisant d'une part, à de possibles abus d'éviction, destinés à décourager, retarder ou éliminer les concurrents par des procédés ne relevant pas d'une concurrence par les mérites (élévation artificielle de barrières à l'entrée, clauses d'exclusivité

en précisant toutefois que de telles positions sont susceptibles d'être remises en cause avec la succession des cycles d'innovation sur Internet. Concomitamment à cet sectorielle, l'Autorité de la concurrence avait, à la suite d'une plainte, prononcé des mesures conservatoires à l'encontre du service de publicité en ligne de Google[55] lui enjoignant à bref délai de préciser les conditions de souscription et d'exécution des contrats avec les entreprises de ce secteur selon des conditions claires, objectives et non-discriminatoires, ainsi que les procédures pouvant conduire à la suspension du compte d'un annonceur[56]. A l'issue de ces mesures conservatoires, Google a pris des engagements largement inspirés de ces mesures, qui ont été rendus obligatoires pour une durée de trois ans en France[57]. Une nouvelle enquête sectorielle a été engagée le 23 mai 2016[58] pour évaluer les nouvelles pratiques de marché et le renforcement éventuel des positions depuis 2010.

L'Autorité a également publié deux études sectorielles en collaboration avec d'autres autorités de concurrence européenne : une première étude en décembre 2014, réalisée conjointement avec la *Competition and Market Authority britannique*, sur l'analyse économique des systèmes ouverts et fermés et la concurrence entre plate-formes verticalement intégrées et autres catégories d'acteurs[59], et une seconde, en mai 2016, réalisée conjointement avec le *Bundeskartellamt* allemand[60], sur les données personnelles et leurs enjeux pour l'application du droit de la concurrence.

Dans le secteur de la réservation de l'hôtellerie en ligne, l'Autorité de la concurrence a obtenu de Booking, à la suite d'une plainte des principaux syndicats hôteliers français et du groupe Accor, qu'il prenne l'engagement de modifier ses pratiques commerciales qui étaient susceptibles de réduire l'intensité de la concurrence entre plate-formes et de permettre aux hôtels d'offrir des nuitées de dernière minute ou à une clientèle fidèle à des conditions plus avantageuses. Booking a ainsi modifié sa clause de parité tarifaire et supprimé toute clause

excessives par leur champ, leur durée ou leur portée, obstacles techniques, etc.) et, d'autre part, à de possibles abus d'exploitation, par lesquels un moteur de recherche imposerait des conditions exorbitantes à ses partenaires ou clients, les traiterait de manière discriminatoire ou refuserait de garantir un minimum de transparence dans les relations contractuelles qu'il noue avec eux. L'avis de l'Autorité de la concurrence avait une portée essentiellement pédagogique, visant à permettre aux entreprises concernées de mettre en conformité leur pratique afin d'éviter des contentieux.

55 Décision 10-D-30 du 28 octobre 2010 relative à des pratiques mises en œuvre dans le secteur de la publicité sur Internet.

56 Décision 10-MC-01 du 30 juin 2010 relative à la demande de mesures conservatoires présentée par la société Navx.

57 Google avait indiqué qu'elle appliquerait en pratique ses engagements à l'ensemble des contenus admis sur son service et dans tous les pays concernés par son service.

58 http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=662&id_article=3014&lang=fr

59 http://www.autoritedelaconcurrence.fr/doc/economics_open_closed_systems.pdf

60 http://www.autoritedelaconcurrence.fr/doc/rapport-concurrence-donnees-vf-mai2016.pdf

imposant des obligations de parité en termes de disponibilités de chambres ou de conditions commerciales à des plate-formes concurrentes non seulement à l'égard des plateformes concurrentes mais également des canaux directs hors ligne des hôtels et d'une partie de leurs canaux en ligne[61]. La Suède et l'Italie avaient obtenu des engagements similaires à l'issue d'une coordination entre les trois autorités. Un bilan d'étape de l'efficacité de ces engagements a été publié en février 2017[62], avant qu'il ne donne lieu à un rapport d'évaluation avec huit autres autorités[63] sous l'égide de la Commission européenne[64] en avril 2017.

2. Médias numériques

Question 2.1.

La position de la Cour de justice de l'Union européenne sur les «frontières» des SMAD est accueillie de façon ambivalente en droit français: la solution est à la fois attendue et porteuse d'insécurité juridique.

Le droit français des SMAD se caractérise par une double complexité: la première source de difficulté concerne la définition même des SMAD car si ces derniers ont été intégrés depuis la loi du 5 mars 2009 dans le champ de compétence du régulateur (CSA), l'article 2 alinéa 6 de la loi du 30 septembre 1986[65], complétée par le I de l'article 1er décret nº2010-1379 du 12 novembre 2010 comporte des carences. La définition française, par ses exclusions – totales[66] ou partielles[67]-

[61] Décision 15-D-06 du 21 avril 2015 sur les pratiques mises en œuvre par les sociétés Booking.com B.V., Booking.com France SAS et Booking.com Customer Service France SAS dans le secteur de la réservation hôtelière en ligne

[62] http://www.autoritedelaconcurrence.fr/doc/bilan_engagements_booking_final_9fev17.pdf

[63] Allemagne, Belgique, Hongrie, Irlande, Italie, Pays-Bas, République tchèque, Royaume-Uni et Suède.

[64] http://ec.europa.eu/competition/ecn/hotel_monitoring_report_en.pdf

[65] Est un SMAD «*tout service de communication au public par voie électronique permettant le visionnage de programmes au moment choisi par l'utilisateur et sur sa demande, à partir d'un catalogue de programmes dont la sélection et l'organisation sont contrôlées par l'éditeur de ce service*»

[66] Loi 1986: «*Sont exclus les services qui ne relèvent pas d'une activité économique au sens de l' article 256 A du code général des impôts, ceux dont le contenu audiovisuel est secondaire, ceux consistant à fournir ou à diffuser du contenu audiovisuel créé par des utilisateurs privés à des fins de partage et d'échanges au sein de communautés d'intérêt, ceux consistant à assurer, pour mise à disposition du public par des services de communication au public en ligne, le seul stockage de signaux audiovisuels fournis par des destinataires de ces services et ceux dont le contenu audiovisuel est sélectionné et organisé sous le contrôle d'un tiers. Une offre composée de services de médias audiovisuels à la demande et d'autres services ne relevant pas de la communication audiovisuelle ne se trouve soumise à la présente loi qu'au titre de cette première partie de l'offre*».

[67] Décret 2010: Art. 1 *II: «Les dispositions du présent chapitre relatives à la contribution au développement de la production d'œuvres cinématographiques ne sont pas applicables aux services qui proposent annuellement moins de 10 œuvres cinématographiques de longue durée. III. – Les dispositions du présent chapitre relatives à la contribution au développement de la production d'œuvres audiovisuelles ne sont pas applicables : 1º Aux services de télévision de rattrapage ; 2º Aux autres services de médias audiovisuels à la demande dont l'offre est principalement consacrée aux programmes mentionnés au cinquième alinéa de l'article 1609 sexdecies B du code général des impôts ou qui proposent*

est difficilement opérationnelle par les opérateurs, source de contentieux[68]. La seconde source de complexité est l'instabilité de leur régime juridique. La France est passée d'un régime d'autorisation préalable –inefficace- à un système de déclaration par la loi nº2013-1028 du 15 novembre 2013 relative à l'indépendance de l'audiovisuel public (art. 34 de la loi du 30 septembre 1986 mod.) avec des obligations juridiques diversifiées (pluralisme culturel, protection des mineurs etc.)[69]. Censé être *a priori* plus souple, et donc plus efficace, il demeure encore en pratique peu effectif comme le souligne le CSA qui «*ne peut être assuré que la totalité des éditeurs lui ont déclaré leur activité*»[70], et souligne le «*caractère lacunaire de nombreuses déclarations*». Le CSA appelle donc à une refonte du statut et du régime juridique des SMAD[71]. Dès lors, il apparait exagéré de parler de «déviance» entre les positions françaises et européenne, même si, en l'état actuel du droit français, il est possible d'évoquer une lecture plus extensive des SMAD par la CJUE. Cette jurisprudence pourrait être une opportunité pour le droit français en élargissant le périmètre des SMAD.

Cette évolution présente toutefois deux risques principaux. Le premier est d'imposer au régulateur national un périmètre d'action plus important, avec les risques contentieux afférents[72], sans que la question de l'adaptation des moyens (juridiques, matériels, humains) du régulateur soit résolue, et ce dans un contexte général en France de défiance vis-à-vis de ce modèle de régulation[73]. Le second serait de se cantonner à une définition des SMAD-avec le risque d'une obsolescence rapide de la définition face aux évolutions technique et aux usages- et de laisser de côté la question essentielle de leur régime juridique: faut –il un alignement par rapport aux média traditionnels ou un régime juridique *sui generis*, inspirés –alignés?- de la régulation à venir des contenus audiovisuels en ligne (Youtube etc)?. Or, en France au-delà des objectifs classiques assignés aux SMAD

annuellement moins de 10 œuvres audiovisuelles autres que celles mentionnées au cinquième alinéa de l'article 1609 sexdecies B du code général des impôts.

[68] CSA, Etude, 29 mai 2013, *Décision de qualification juridique des vidéos en libre accès sur les sites internet des radios en SMAD*

[69] CSA, délibération du 20 décembre 2011, *Protection du jeune public, à la déontologie et à l'accessibilité des programmes sur les services de médias audiovisuels à la demande*

[70] http://www.csa.fr/Etudes-et-publications/Les-autres-rapports/Rapport-au-Gouvernement-sur-l-application-du-decret-n-2010-1379-du-12-novembre-2010-relatif-aux-services-de-medias-audiovisuels-a-la-demande-SMAD

[71] CSA, 2016: *Les effets économiques du décret nº 2010-1379 du 12 novembre 2010 relatif aux services de médias audiovisuels à la demande*

[72] CSA, Assemblée plénière, 12 juillet 2017, *Diffusion de bandes-annonces déconseillées aux moins de 10 ans en amont de dessins animés pour jeunes enfants sur MyTF1*

[73] V. not. Sénat, Rapport d'information nº 371 (2003-2004) *Le Conseil supérieur de l'audiovisuel : Garantir les moyens d'une ambition*; Commission d'enquête, Rapport nº126 (2015-2016) 28 octobre 2015, *Un État dans l'État : canaliser la prolifération des autorités administratives indépendantes pour mieux les contrôler*

(déontologie, protection des mineurs), d'autres finalités sont poursuivies liées à l'exception culturelle (production et de promotion des œuvres européennes et d'expression originale française), qui pourraient ne pas être reprises dans la directive.

Ainsi, dans un souci de sécurité juridique il serait préférable que la position de la CJUE soit «codifiée» à l'occasion de la révision de la directive SMA afin d'unifier les définitions nationales, disparates, et d'identifier clairement le périmètre des SMAD dans leur «pluralité», à même de fonder l'élaboration d'un régime juridique harmonisé, sous l'égide de l'ERGA par la définition de «bonnes pratiques» (*guidelines*) associant régulateurs nationaux et acteurs concernés (*Self and coregulation*).

Question 2.2.

Pour répondre à cette question, sensible, il convient de partir du droit français des médias qui se caractérise par son ambivalence: si la question de régulation publique des plateformes vidéo suscite de nombreux rapports, notamment du régulateur audiovisuel national[74], aucun texte récent intervenu dans le secteur audiovisuel ne fonde de façon expresse l'intervention du CSA[75], ce dernier se heurtant à leur statut de simples «hébergeurs», et non d'«éditeurs»[76].

Dès lors si les plateformes de vidéo tendent à être régulées, c'est par la voie d'autres textes –et d'autres modalités, régulateurs – n'ayant pas pour objectifs ceux spécifiques de la régulation des médias (déontologie, pluralisme, publicité et parrainage etc.). Il s'agit de textes soit sectoriels (ex. terrorisme[77]), soit généraux comme la loi nº2016-1321 du 7 octobre 2016 sur la «République numérique» consacrant notamment un principe général de loyauté des plateformes en ligne –dont celles de partage de vidéos. La difficulté est que le CSA est *a priori* exclu du contrôle prévu dans la loi au profit d'autres acteurs ou régulateurs publics.

Reste que le régulateur audiovisuel national tente néanmoins d'intervenir, même sans assise juridique explicite, pour répondre au besoin du public et des éditeurs historiques comme en témoignent les vœux de son Président en 2017 : «*Pas un jour ne se passe sans que nous soyons interpellés sur notre rôle de protection des publics, notamment des plus fragiles, sur les supports numériques (...) nous sommes sou-*

[74] CSA, 8 décembre 2016, *L'audiovisuel dans l'espace numérique : plateformes et données*

[75] V. not. Loi nº 2016-1524 du 14 novembre 2016 *visant à renforcer la liberté, l'indépendance et le pluralisme des médias*

[76] Cf. art. 14 de la Directive 2000/31/CE et art. 6-I-2 de la loi nº2004-575 du 21 juin *2004 pour la confiance dans l'économie numérique*

[77] Article 20 de la loi nº 2016-987 du 21 juillet 2016 *prorogeant l'application de la loi du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste*, ayant complété l'article 15 de la loi du 30 septembre 1986 mod.; v. aussi CSA, 25 octobre 2016, *Précautions relatives à la couverture audiovisuelle d'actes terroristes*

vent le réceptacle des indignations de nos concitoyens, qui ont le réflexe naturel de se tourner vers nous. Le public n'est d'ailleurs pas le seul à nous interpeller, puisque les éditeurs se plaignent à juste titre également des «asymétries» dans la régulation que nous opérons»[78]. Le CSA pour répondre à cette double attente a créé des groupes de réflexion («Rencontres du CSA», «CSA Lab»), mais a aussi, pour la première fois, par une décision du 9 novembre 2016 appliqué le régime des SMAD à une plateforme vidéo en considérant l'opérateur comme un «éditeur du service». Or, en raison de très nombreuses références à l'alcool dans le programme litigieux, le CSA a «mis en garde» l'opérateur contre le renouvellement d'un tel manquement[79], avec toutefois une efficacité plus que relative en pratique[80]...

Dès lors, si l'extension du périmètre de la directive SMA auxdites plateformes s'inscrit dans une «bonne direction», elle présente aussi des risques car elle soulève de nombreuses interrogations qui actuellement ne sont pas résolues par le droit français :

- Quel est le niveau pertinent de régulation (national, européen)? Quel mode de régulation (publique et/ ou privée)? Quels seront les dispositifs de collaboration entre les diverses autorités de régulation compétentes (secteurs audiovisuel, des données personnelles, des communications électroniques mais aussi aspects concurrentiels)? La création d'une autorité de régulation nationale et/ou européenne de la communication serait-elle faisable? acceptable en opportunité?
- Quel doit être leur statut juridique (hébergeur, éditeur, ou *sui generis*?)
- A quelles obligations doivent être tenus ces nouveaux opérateurs, et: obligations *sui generis*, plus souples que celles des médias traditionnels,ou alignement sur celles des SMAD? Dès lors, quelles conséquences sur les obligations pesant sur les médias historiques ? Doivent-elles être «allégées» pour corriger les asymétries de régulation avec les nouveaux entrants, afin de favoriser une concurrence loyale (ex. proposition dans la révision de la directive SMA d'allègement des règles relatives aux communications commerciales)?
- Au-delà des objectifs consensuels et *a minima* de protection des mineurs, et des règles relatives à la communication commerciale, *quid* des objectifs spécifiques de la régulation des médias dont la déontologie des médias et le principe de pluralisme (politique, social, cultuel), la représentation de

[78] http://www.csa.fr/Espace-Presse/Interventions-publiques/Discours-d-Olivier-Schrameck-a-l-occasion-de-la-presentation-des-voeux-2017-du-Conseil

[79] CSA, 9 novembre 2016, "*Les Recettes Pompettes by Poulpe» sur YouTube.*

[80] V. not. l'insertion d'avertissement dans les vidéos: https://www.youtube.com/watch?v=-yhobPj8DZc ou https://www.youtube.com/watch?v=r50WOoW95G8

la diversité, le respect de la dignité humaine, l'égalité femmes-hommes etc (art. 1er de la loi du 30 septembre 1986), et notamment quel devenir pour les dispositifs juridiques de protection de la création artistique indépendante (quotas de production/diffusion etc)?

Ainsi, l'extension du périmètre de la directive SMA aux plateformes vidéo comporte des ambiguïtés car la logique de régulation qui prédomine demeure *a minima* – en raison du statut juridique ambigu des plateformes vidéo, à la croisée de différentes législations nationales et européennes- et ce processus s'accompagne d'une logique de dérégulation des médias historiques (révision des règles relatives à publicité et au parrainage). Or, il peut en résulter une «banalisation» des objectifs spécifiques de la régulation de médias; à la régulation audiovisuelle s'ajoute en effet de plus en plus une régulation fondée sur d'autres objectifs, qui peuvent rejoindre celui du pluralisme culturel. Ainsi, la régulation concurrentielle peut indirectement participer de la régulation audiovisuelle, comme en témoigne notamment en droit français les décisions de l'Autorité de la concurrence relatives aux injonctions imposées au Groupe Canal Plus[81].

Question 2.3.

La question de la compétence territoriale est essentielle pour la France qui s'est dotée d'un arsenal législatif et réglementaire visant à favoriser la diversité culturelle, à soutenir la création, qui engendre des obligations pour les opérateurs de services de médias audiovisuels auxquelles il peut être tentant d'échapper. Le maintien du principe du pays d'origine (PPO) sans aménagement présente ainsi le risque d'une concurrence inéquitable entre opérateurs établis en France et hors du pays et celui d'une remise en cause de l'efficacité du dispositif français. Le mécanisme prévu à l'heure actuelle par la directive SMA (article 4.2), qualifié de dispositif anti-contournement, qui permet à l'Etat membre de destina-

[81] Décision nº17-DCC-92 du 22 juin 2017 *portant réexamen des injonctions de la décision nº12-DCC-100 du 23 juillet 2012 relative à la prise de contrôle exclusif de TPS et CanalSatellite par Vivendi SA et Groupe Canal* http://www.autoritedelaconcurrence.fr/pdf/avis/17DCC92versionpublication.pdf. Cette décision s'inscrit dans un ensemble remontant à 2005. Lors de sa fusion avec son concurrent TPS, le groupe Canal Plus avait souscrit des engagements permettant à préserver la concurrence tant sur le marché amont de l'acquisition de certaines catégories de droits (œuvres cinématographiques acquises auprès des grands studios des Etats-Unis, œuvres d'expression française, droits sportifs notamment) que sur le marché aval de la distribution. Faute d'exécution de ces engagements, l'Autorité de la concurrence a enjoint en 2012, au regard des conditions de marché qui prévalaient alors, des mesures encadrant le comportement de Canal plus, sans cependant affecter les obligations à la charge du groupe de financement du cinéma français ou remettre en cause la chronologie des médias, qui ne relevaient pas de sa compétence. La décision de 2017 met à jour ces injonctions au regard des évolutions de marché depuis lors intervenues, notamment en ce qui concerne la vidéo à la demande (entrée d'Altice, Netflix et Amazon sur le marché)

tion d'imposer des obligations aux opérateurs établis dans un autre Etat membre mais fournissant une émission télévisée destinée entièrement ou principalement à son territoire, apparaît à cet égard insuffisant. Ce dispositif est très complexe à mettre en œuvre et insuffisant pour répondre aux effets pervers du PPO.

Le législateur français a été plus ambitieux que la directive. Il a intégré ce mécanisme dans la loi du 30 septembre 1986 en l'étendant aux SMAD (article 43-10 de la loi du 30 septembre 1986 mod.[82] et décret nº 2010-1593 du 17 décembre 2010[83]) contrairement à ce que prévoit la directive, ce qui n'est pas approuvé par la Commission européenne[84]. En outre, le dispositif en France vise à amener l'organisme délocalisé à respecter «*l'ensemble de la législaton française*» et non seulement «*les règles d'intérêt public général*».

Cependant, même si l'introduction de ce mécanisme dans la directive SMA répond à des préoccupations notamment des autorités françaises[85], l'utilisation de ce dispositif est assez illusoire car, comme le note le CSA, il est difficile «*d'établir que la programmation d'un service est «entièrement ou principalement» destinée au public français [...] ce pourquoi* [le dispositif «anti-contournement»] *n'a in fine jamais été mis en oeuvre*»[86]. En tout état de cause, même si ce mécanisme peut servir à contraindre des opérateurs contournant la législation d'un Etat membre, il ne permet pas de couvrir toutes les hypothèses de *forum shopping* réglementaire et fiscal, le fournisseur choisissant l'Etat membre dans lequel les réglementations et la fiscalité sont les plus souples tout en diffusant ses services dans différents autres Etats membres. Cette hypothèse se pose tout particulièrement dans le cas des SMAD type SVOD dont la programmation est plus universelle et à même

[82] Article 43-10 : "Si *un service de télévision ou un service de médias audiovisuels à la demande dont la programmation est entièrement ou principalement destinée au public français s'est établi sur le territoire d'un autre Etat membre de la Communauté européenne ou partie à l'accord sur l'Espace économique européen dans le but principal d'échapper à l'application de la réglementation française, il est réputé être soumis aux règles applicables aux services établis en France, dans des conditions fixées par décret en Conseil d'Etat.*»

[83] *JORF* nº 0294 du 19 décembre 2010, texte nº 29, p. 22 368.

[84] Voir P. Lescure, *Mission Acte II de l'exception culturelle, Contribution aux politiques culturelles à l'ère numérique*, mai 2013, Fiche A-9, p. 149.

[85] Avant la révision de la directive en 2007, des cas probables de contournement n'ont pas pu être résolus, la France étant tenue de se soumettre aux critères de détermination de la compétence de l'Etat d'origine et au PPO (voir le cas de la société RTL 9 établie au Luxembourg (Conseil d'Etat, 25 novembre 1998, *Société CLT*, *Rec.* p. 443) et une décision du 9 mai 2006, par laquelle le CSA, saisi par le SPI (Syndicat des producteurs indépendants), la SACD et le CSPF (Chambre syndicale des producteurs de films), a estimé que la chaîne Fox Life, bien que diffusant en France, était bien établie en Italie, les décisions stratégiques étant adoptées dans ce dernier pays (http://www.csa.fr/Espace-juridique/Decisions-du-CSA/Situation-de-la-chaine-Fox-Life-le-Conseil-repond-a-la-SACD-au-SPI-et-a-la-CSPF).

[86] CSA, 3 novembre 2015, *Réponse à la consultation de la Commission européenne sur la directive Services de médias audiovisuels – Un cadre pour les médias du 21ème siècle*, p. 37, http://www.csa.fr/%20csa/Le-CSA/Europe-et-international/Reponse-du-CSA-a-la-consultation-de-la-Commission-europeenne-sur-la-directive-Services-de-medias-audiovisuels-Un-cadre-pour-les-medias-du-21e-siecle

d'intéresser des publics divers de différents Etats membres que celle des services linéaires classiques.

Les autorités françaises ont montré leur désir de s'emparer de la question et de réagir en souhaitant étendre une taxe de 2%[87] sur les recettes générées par la vente et la location de vidéos et, par assimilation, la mise à disposition de services payants offrant l'accès à des œuvres cinématographiques et audiovisuelles sur demande individuelle aux fournisseurs de services payants de VOD établis hors de France (dite «taxe Netflix»[88]) puis – en élargissant l'assiette de la taxe aux recettes publicitaires – aux plateformes gratuites permettant l'accès à des oeuvres cinématographiques et audiovisuelles (dite «taxe YouTube»[89]). Ce type de mesure vise à déroger au PPO pour tenir compte du pays de destination, de «l'établissement du service»[90], et nécessite bien évidemment une approbation de la part de la Commission européenne qui semble à l'heure actuelle en avoir une aproche assez favorable[91]. Ceci peut être salué malgré les limites de tels mécanismes (difficulté de recouvrement, caractère dérisoire des recettes...) et le manque d'ambition de la proposition de directive à ce propos (limitation aux SMAD et à l'obligation de contribution à la production).

Le PPO n'est pas remis en cause dans son principe, notamment par le CSA. Mais des aménagements sont requis et seraient bienvenus, en particulier un engagement plus fort de l'UE dans l'imposition de mesures plus volontaristes que celles envisagées (quotas notamment) en faveur de la diversité culturelle[92].

Questions 2.4. et 2.5.

Le paysage européen des «régulateurs» audiovisuels nationaux est extrêmement disparate. La numérisation des médias peut être à l'origine *a priori* d'un «pas en avant» *via* une harmonisation des pratiques nationales concernant leur «indépen-

[87] Portée à 10 % si le service propose des oeuvres à caractère pornographique ou incitant à la violence.

[88] Article 30 IV B de la loi de finances rectificative pour 2013 (loi nº 2013-1279 du 29 décembre 2013, *JORF* nº 0303 du 30 décembre 2013, texte nº 2, p. 21910)

[89] Article 56 de la loi nº 2016-1918 du 29 décembre 2016 de finances rectificative pour 2016, *JORF* nº 0303 du 30 décembre 2016, texte nº 2

[90] Critère proposé par le rapport Lescure précité.

[91] Dans sa proposition de révision de la directive SMA en mai 2016, la Commission propose de permettre aux Etats membres d'imposer à un SMAD établi dans un autre Etat membre mais ayant des clients sur leur territoire une obligation de contribution à la production d'oeuvres européennes à condition qu'une telle contribution ne soit pas déjà versée dans l'Etat d'origine ; voir aussi la décision de la Commission du 1er septembre 2016 autorisant ce type de taxes en Allemagne (https://www.lesechos.fr/tech-medias/medias/030552474606-bruxelles-a-dit-oui-aux-taxes-youtube-et-netflix-2113639.php)

[92] http://www.csa.fr/Etudes-et-publications/Autres-publications-syntheses-de-consultations-et-de-concertations-reponses-aux-pouvoirs-publics-comptes-rendus-de-missions-et-d-auditions-etc/Position-du-Conseil-superieur-de-l-audiovisuel-sur-la-proposition-de-la-Commission-europeenne-visant-a-reviser-la-directive-Services-de-medias-audiovisuels

dance». La question que l'on peut néanmoins se poser est de savoir si ce modèle de régulation est encore celui qui est adapté aux mutations du secteur. Cette consécration européenne n'est-elle pas trop tardivevoire «dangereuse» pour la création d'un marché unique de l'audiovisuel numérique? Le droit des médias français témoigne de tous ces questionnements. Ainsi en est-il de la fragilité de la création – et du maintien – de l'existence d'un régulateur sectoriel indépendant en France. Depuis la suppression du monopole étatique en 1982[93], et la création de la première instance de régulation (HACA), pas moins de trois instances, toutes «indépendantes» en vertu de la loi, se sont succédées (HACA, CNCL[94], CSA[95]) révélant les «pressions politiques» – et parfois «commerciales»- qui ont été exercées sur ces différentes instances, et leur quête difficile d'indépendance.

De même, la longévité du CSA, crée en 1989, ne doit pas masquer ses profondes mutations, car le CSA actuel -devenu en 2013 une autorité publique indépendante (API) dotée de la personnalité morale de droit public[96]- n'est plus celui des origines : tant sa composition, que son organisation, son statut et ses pouvoirs ont été profondément modifiés par les textes, et ce notamment sous l'influence de la jurisprudence nationale et européenne sur l'indépendance et impartialité du CSA dans l'exercice de ses fonctions répressives[97]. Le CSA a donc dans la période récente connu des fluctuations importantes, dont certaines ont pu être considérées comme des atteintes à son indépendance (2009), sur lesquelles des lois de 2013 sont revenues[98]. Si le CSA dispose bien entendu d'une large compétence en matière de régulation, une interrogation se fait jour quant à la limitation de la portée de son pouvoir réglementaire[99], le juge constitutionnel ayant reconnu, de façon générale, une exclusivité réservée au Premier ministre par l'article 37 de la Constitution, qui ne peut faire l'objet au bénéfice de régulateurs indépendant que pour une délégation de portée limitée, tant dans son objet que par son contenu[100].

[93] Loi nº 82-652 du 29 juillet 1982 sur la communication audiovisuelle.

[94] Loi nº 86-1067 du 30 septembre 1986 relative à la liberté de communication.

[95] Loi nº 89-25 du 17 janvier 1989 modifiant la loi nº 86-1067 du 30 septembre 1986 relative à la liberté de communication.

[96] Loi nº 2013-1028 du 15 novembre 2013 relative à l'indépendance de l'audiovisuel public.

[97] V. not. l'alignement du pouvoir répressif du CSA sur le modèle de l'Adlcpar la loi nº 2013-1028 du 15 novembre 2013 mod. l'article 42-7 la loi nº 86-1067 du 30 septembre 1986.

[98] La loi nº 2009-258 du 5 mars 2009 relative à la communication audiovisuelle et au nouveau service public de la télévision avait retiré au CSA le pouvoir de nomination des dirigeants de l'audiovisuel public pour le confier au président de la République. Les lois ordinaire et organique relatives à l'indépendance de l'audiovisuel public, adoptées le 15 novembre 2013, ont réattribué cette compétence au CSA.

[99] c'est-à-dire d'exécution des lois ou de réglementation dans des matières qui ne sont pas réservées au législateur, et n'affectent ainsi pas la liberté du commerce et de l'industrie.

[100] Conseil constitutionnel, décision nº 88-248 DC du 17 janvier 1989 en vertu de laquelle la Constitution confère au «*Premier ministre, sous réserve des pouvoirs reconnus au Président de la République, l'exercice du pouvoir*

Si la révision directive SMA devrait permettre de consacrer le «modèle» d'une régulation sectorielle indépendante, elle devrait aller au-delà du simple «label» d'indépendance, pour en préciser le contenu car des libertés fondamentales sont en jeu, et constituent les bases de la démocratie (liberté d'expression, pluralisme politique etc). Le statut d'autorité publique indépendante acquis par le CSA en 2013 et 2017 et les lois organique et ordinaire nº2017-54 nº2017-55 du 20 janvier 2017 relatives aux autorités administratives indépendantes et aux autorités publiques indépendantes pourraient ainsi être d'une utile inspiration: garanties d'indépendance et d'impartialité, affirmation du principe de collégialité, de la réserve et du secret des délibérations, précision accrue de la procédure de nomination, des critères de compétence et des règles déontologiques (dépôt de déclarations d'intérêts et de patrimoine, avec contrôle interne et externe, incompatibilités électorales, contrôle des activités professionnelles des membres et anciens membres avec des règles d'incompatibilités professionnelles durant le mandat et au sortir du mandat), diversification des autorités de nomination, encadrement de la durée et de l'exercice du mandat (caractère non renouvelable, l'exercice à temps pleindu mandat, l'interdiction du «cumul des mandats», notamment entre organismes de régulation), contrôle démocratique du Parlement de l'action du régulateur (ex. rapport annuel, publicité des avis), un contrôle juridictionnel indépendant et efficace de l'action du régulateur.

L'indépendance du régulateur audiovisuel suppose aussi par celle des services administratifs, dont les agents doivent aussi être soumis à des règles déontologiques définies par le régulateur (règlement intérieur, code de déontologie); le régulateur sectoriel doit donc bénéficier d'un statut juridique lui permettant une autotomie de gestion, comme celui d'API du CSA attribué en 2013.

In fine, une question se pose : cette carence de la directive SMA doit-elle être comblée ? En effet, l'utilité même d'un régulateur sectoriel audiovisuel en France est régulièrement posée en France, la fusion ou le rapprochement du CSA avec d'autres régulateurs sectoriels dont les champs de compétences se chevauchent (CSA, ARCEP, CNIL, HADOPI, CADA,...) étant proposé[101]. Cela résulte de la convergence numérique et de la prédominance des logiques concurrentielles. La création d'un marché unique de l'audiovisuel européen numérique pourrait même être fragilisée par la consécration de l'indépendance du régulateur sectoriel, celui-ci pouvant apparaitre comme un facteur de résistance par la pré-

réglementaire à l'échelon national ; que si elles ne font pas obstacle à ce que le législateur confie à une autorité de l'État autre que le Premier ministre le soin de fixer des normes permettant de mettre en oeuvre une loi, c'est à la condition que cette habilitation ne concerne que des mesures de portée limitée tant par leur champ d'application que par leur contenu».

[101] V. not. les rapports parlementaires: P. Gelard, *Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié, 2006*; Comité d'évaluation et de contrôle des politiques publiques, *Les autorités administratives indépendantes : pour une indépendance sous la garantie du Parlement*, 2010.

valence donnée aux logiques non concurrentielles. D'autres pistes pourraient être envisagées, car les médias numériques supposent la recherche de nouvelles formes de régulation, reposant sur des logiques de «co-» ou «interrégulation» publiques -avec une approche «transversale» de la communication et un partenariat étroit avec le régulateur concurrentiel – et privées (auto-régulation des opérateurs). En outre, l'officialisation de l'ERGA par la révision de la directive SMA suppose aussi de garanties quant à son indépendance vis-à-vis des institutions européennes et nationales[102].

Question 2.6.

La pratique de la publicité ciblée a été engagée en France par les opérateurs audiovisuels (nouveaux entrants et médias historiques dont TF1, *via* la *catch up tv*) suscitant des controverses sur la protection des données personnelles et de la vie privée. Les réponses des régulateurs (CSA, CNIL) ont été timides, en raison d'un hiatus entre l'état du droit français qui exclut la possibilité du ciblage dans les médias audiovisuels «classiques» (article 13 du décret nº 92-280 du 27 mars 1992 modifié) et les pratiques des opérateurs, et notamment des nouveaux entrants. Les initiatives normatives des régulateurs demeurent encore limitées (Délibération CNIL; CSA, Rapport, 4 novembre 2016: *Les nouveaux territoires publicitaires : quels enjeux pour la télévision ?*), et ne reflétant pas de réelles coopérations –du moins officielles – des régulateurs, initiatives complétées par des acteurs privées (Recommandation ARPP; Charte UFMD).

Le contexte législatif national relatif à la publicité digitale a récemment évolué (article 131 de la loi nº 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques modifiant l'article 23 de la loi nº 93-122 du 29 janvier 1993 relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publique pour les nouvelles pratiques des entreprises de la publicité digitale, qui orientent notamment les messages vers des destinataires ciblés en temps réel, dans le cadre d'enchères), et *via* le décret nº 2017-159 du 9 février 2017 relatif aux prestations de publicité digitale.

Ainsi, reste un régime juridique encore parcellaire, et qui pose la question du(des) régulateur(s) compétent(s) – et de leur coopération- pour en assurer le respect. La régulation nationale «éclatée» (publique: CNIL, CSA, et privée: ARPP) fonde la nécessité d'une harmonisation européenne (contrôle notamment) afin de conforter et développer des «bonnes pratiques» fondées sur une corégulation public/privé.

[102] V. not. l'article 30bis relatif à l'ERGA de la directive du Parlement européen et du Conseil COM(2016) 287 final modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels, compte tenu de l'évolution des réalités du marché.

Question 2.8.
Les restrictions contractuelles qui confèrent une exclusivité à un distributeur ou un fournisseur sont la résultante de l'écosystème du financement des œuvres audiovisuelles.

Dans le domaine audiovisuel, à la différence de la musique, au demeurant déjà régie par un cadre européen récent, la directive 2014/26/UE, la demande portant sur des offres transfrontalières ne porte que sur une proportion très réduite de contenu pour lesquels se justifie une exploitation à l'échelle paneuropéenne. Les acteurs du secteur devraient donc demeurer libres d'adapter leurs pratiques contractuelles à une demande qui comporte une forte dimension locale, liée aux goûts des consommateurs et à la maîtrise ou non des langues.

Les effets bénéfiques/pro-concurrentiels liés aux exclusivités territoriales sont largement documentés y compris par des études d'économistes renommés commandées par la Commission européenne elle-même (étude Charles Rivers Associates notamment) ou plus récemment par les titulaires de droits (étude Oxera). En effet, confier un droit d'exploitation exclusif à un distributeur lui permet d'entreprendre des efforts de promotion de l'œuvre sans craindre qu'un concurrent qui n'a pas supporté ces investissements n'en retire les fruits[103]. De même, l'exclusivité territoriale permet de répondre à la diversité culturelle et à une logique d'amortissement des investissements et d'un bénéfice raisonnable eu égard aux risques pris. Enfin et surtout, l'exclusivité accordée au distributeur lui garantit des revenus suffisants pour qu'il accepte, à l'avance, de soutenir financièrement la création par le mécanisme des préventes. L'exclusivité permet en particulier de rémunérer le risque pris sur une œuvre qui n'est pas d'emblée promise à une audience de portée mondiale.

Pour prendre l'exemple du Royaume-Uni, étudié dans l'analyse d'Oxera, à peine 6,6% des films indépendants produits sont rentabilisés à hauteur de deux fois leur budget de tournage deux ans après leur sortie en salle. Les pré-ventes, que seule l'exclusivité territoriale garantit, représentent plus de 50% des financements de the Cut, 45% de The Lobster, 28% de Amour.

C'est la raison pour laquelle, tout en remédiant aux difficultés de portabilité d'un abonnement pour un public peu nombreux mais fortement demandeur,

[103] Le distributeur est ainsi incité à assurer une promotion adéquate de l'œuvre, tenant compte des spécificités culturelles locales, sur son territoire exclusif. En effet, les produits culturels sont des biens d'expérience, et la demande doit être stimulée par des efforts de contextualisation qui donneront au public envie de découvrir l'œuvre. En outre, dans le secteur audio-visuel, et plus encore pour les films d'auteur,le succès commercial d'une œuvre dépend largement des efforts d'adaptation au marché local, notamment par le doublage/sous-titrage et une promotion adaptée au contexte culturel. Il y a peu d'économies d'échelle à opérer ces efforts à une dimension multinationale. Les investissements se font donc à l'échelle nationale (voire à l'échelle d'une zone linguistique regroupant quelques pays), et les licences sont accordées sur une base exclusive nationale.

le consommateur qui se déplace très régulièrement (résidents transfrontaliers, personnes qui font régulièrement des déplacements intra-européens) et ne peut en bénéficier pleinement alors qu'il souscrit un abonnement légal dans son pays d'origine, il serait risqué, pour les œuvres ne touchant qu'un public essentiellement national, pour des raisons culturelles et linguistique, de remettre en cause la portabilité des droits. En revanche, la portabilité temporaire peut être consentie sans déstabiliser les circuits de financement car le consommateur reste ciblé par les efforts de promotion dans son pays d'origine.

Pour tracer cette limite, un contrôle régulier est nécessaire, dans le respect des législations européennes et nationales sur la protection des données. Les données en question ne sont pas celles de la localisation précise de l'abonné, ce qui constituerait en effet une ingérence disproportionnée; le critère retenu serait purement «binaire» : l'abonné accède-t-il à l'offre à partir de son Etat membre de résidence ou d'un autre Etat?

4. Données dans l'économie numérique

Question 4.1.

La réforme de la protection des données personnelles s'est accompagnée en France de travaux de réflexion préalables (étude annuelle du Conseil d'Etat de 2014 sur le Numérique et les droits fondamentaux[104], rapport au Président de l'Assemblée nationale de la commission de réflexion sur le droit et libertés à l'âge numérique en octobre 2015), et de premières étapes législatives avec l'adoption de la loi précitée pour une République Numérique du 7 octobre 2016, à l'issue d'un processus d'adoption original incluant une consultation participative. Elle a anticipé l'adoption du RGPD en incluant notamment une première référence au droit à l'oubli numérique, un droit à la portabilité des données et une augmentation les pouvoirs de l'autorité de protection des données la CNIL (notamment le montant des sanctions qu'elle peut infliger en attendant l'application du RGPD). En outre, l'article 65 de cette loi prévoyait la remise d'un rapport le 30 juin 2017 pour préparer les modifications nécessaires de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Enfin, la préparation de l'entrée en vigueur du RGDP a fait l'objet d'une mission d'information qui à la suite d'auditions a rendu un rapport[105] sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française adopté le 22 février 2017. Ce document comporte une première analyse de la réforme européenne de la protection des données personnelles et

[104] http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf

[105] http://www2.assemblee-nationale.fr/documents/notice/14/rap-info/i4544/(index)/rapports-information

des mesures nationales à prendre qu'elle implique. Un projet de loi devrait être prochainement déposé au Parlement.

Question 4.2.
Plusieurs enquêtes circulent attestant globalement que toutes les entreprises ne sont pas prêtes. Selon le livre Blanc[106] publié en juin 2017 par IDC «9% d'entre elles se disent aujourd'hui conformes aux dispositions du GDPR. Elles sont par ailleurs 19% à planifier les initiatives à mettre en place pour être conforme avant la fin 2017 tandis que 30% ont prévu les actions nécessaires pour une mise en conformité courant 2018. En définitive, près d'1 entreprise sur 2 (42%) prend tout juste conscience de l'existence du GDPR et du calendrier associé sans avoir véritablement commencé à lancer des initiatives. Ce phénomène est encore plus important au sein des PME (entreprises disposant de 500 à 1 000 collaborateurs) et des entreprises du secteur privé qui sont respectivement 47% et 46%à «découvrir» les dispositions prévues par le GDPR.». La plupart des entreprises doutent de leur capacité à être en conformité avec le RGPD d'ici mai 2018. «Seules 28% des structures interrogées estiment qu'elles le seront sans aucun doute possible tandis qu'à l'opposé, 27% ont la quasi-certitude qu'elles ne pourront pas l'être. Entre les deux extrêmes, 44% espèrent être le plus alignées possible sans pour autant avoir la conviction d'y arriver». Ces études ou prises de position alarmistes peuvent néanmoins être orientées car elles sont le plus souvent réalisées, soit par des cabinets d'avocats, soit par des entreprises impliquées dans le conseil pour se mettre en conformité avec le RGPD.

Lors de conférences publiques, la CNIL (Commission Nationale Informatique et Liberté, autorité française de contrôle) signale régulièrement le retard pris par les entreprises pour préparer la mise en conformité.

Question 4.3.
Parmi les nombreuses questions qui font débat on retiendra:

- Celle de savoir si le RGPD permet véritablement de répondre à ses objectifs notamment est-il adapté aux usages et à la technologie
- Celle des atteintes potentielles des personnes liées au ciblage, profilage. L'installation par exemple des compteurs électriques intelligents Linky a donné lieu à une vaste campagne en vue du dépôt d'une action de groupe fondée notamment sur les risques au regard de la protection de la vie privée que présenteraient en temps réel la connaissance détaillée de leur consommation électrique. (des enjeux de santé publique sont aussi évoqués).

[106] http://www.juniper.net/assets/fr/fr/local/pdf/whitepapers/idc-gdpr-etude-france-2017.pdf

– D'autres questions font l'objet de débats doctrinaux:
  • Faut-il ou non un droit des robots?
  • Doit-on organiser un régime de propriété des données?

Question 4.4.
La France constitue le pays dans lequel les requêtes de demande déréférencement sont les plus importantes, (130 536 demandes, 48,7% d'URL supprimées au 12 juillet 2017). Il existe une dizaine d'affaires juridictionnelles connues concernant le droit à l'oubli. Pour plus d'information cf. O. Tambou, Trois enseignements à tirer de la mise en œuvre juridictionnelle de l'arrêt Google Spain en France, e-conférence sur le droit à l'oubli en Europe et au-delà, Mai 2017, *Blogdroiteuropeen,* accessible à http://wp.me/p6OBGR-23Z

Le juge judiciaire français est l'arbitre des conflits de déréférencement entre les moteurs de recherche et des particuliers. Une première série de litiges porte sur des refus de Google de déréférencer certaines URL qui ont été examinés en référé par des Tribunaux de Grande Instance (TGI). Chacune de ces ordonnances citent explicitement l'arrêt Google Spain. La plupart estiment que le refus de Google de faire droit au déréférencement demandé par le requérant n'était pas justifié par le droit à l'information légitime du public. Dans ces cas, le juge adresse une injonction de déréférencement à la société Google Inc. et non à la société Google fr. La compétence du juge des référés est néanmoins subordonnée à l'existence d'une demande de déréférencement préalable auprès du moteur de recherche.

Une seconde série d'affaires atteste que le juge judiciaire est le juge protecteur des organes de presse. Le juge judiciaire, et en particulier, la Cour de Cassation considère que la liberté de la presse s'oppose à l'existence d'une obligation des organes de presse de pratiquer un déréférencement dans le moteur interne de leurs archives, voire de supprimer toutes les données personnelles présentes dans celles-ci par un processus d'anonymisation). L'expérience française atteste qu'agir contre un site de presse plutôt que contre un moteur de recherche est plus aléatoire.

De son côté, le Conseil d'État a adressé à la CJUE deux séries de questions préjudicielles (voir supra). La première concerne la portée de l'obligation de déréférencement pesant sur les moteurs de recherche notamment à l'égard de données sensibles et relatives aux condamnations pénales ou aux mesures de suretés, la seconde question préjudicielle étant relative à la portée géographique du déréférencement. Elle s'inscrit dans le contexte de la réponse apportée par la Cour suprême du Canada rendue le 28 juin 2017 dans l'affaire Google Inc. c. Equustek Solutions Inc.[107] par laquelle les juges ont demandé un déréférencement mondial à Google.

[107] https://scc-csc.lexum.com/scc-csc/scc-csc/fr/item/16701/index.do.

GERMANY

Prof. em. Dr. Dr.h.c. Wolfgang Kilian*
Prof. Dr. Benjamin Raue**

In der Europäischen Union sind mit der kommerziellen Nutzung des Internets und der Bereitstellung von Funkfrequenzenelektronische Märkte entstanden. Ihre Vorteile liegen darin, dass Verträge über Waren und Dienstleistungen elektronisch grenzüberschreitend geschlossen und Dienstleistungen grenzüberschreitend elektronisch erbracht werden können. Im Monti-Bericht aus dem Jahre 2010[1], in dem die Bezeichnung „digitaler Binnenmarkt" erstmals auftaucht, werden TK-Dienste, TK-Infrastrukturen, ein gesamteuropäisches Lizensierungssystem, der elektronische Handel sowie Online-Inhalte als Beispiele genannt.

Wegen der grenzüberschreitenden Effekte besitzt die Union die primäre Gesetzgebungskompetenz.[2] Diese wird durch EU-Rahmenregelungen für die Marktstruktur sowie für das Marktverhalten der Kommunikationsbeteiligten wahrgenommen. Inhaltlich richten sich die Rahmenregelungenüberwiegend nach dem Prinzip der „funktionalen Äquivalenz" zu klassischen Marktregelungen, soweit nicht wegen der Besonderheiten der elektronischen Kommunikation neue Instrumente und Verfahren geschaffen werden müssen (etwa: elektronische Signaturen; Datenschutz; Datensicherheit; europäische Clouds).

* Leibniz-Universität Hannover.
** Universität Trier.

[1] Monti, Eine neue Strategie für den Binnenmarkt, S. 54-57 (ec.europa.eu/internal_market/strategy/docs/monti-report_final_10_05_2010_de.pdf), aufgesucht am 6.9.2017.

[2] Padoa-Schioppa, Efficiency, Stability and Equity. A Strategy for the Evolution of the Economic System of the European Community, Oxford 1987; Kilian/Wendt, Europäisches Wirtschaftsrecht, 6.A. 2017, S. 157 ff; 370 ff.

Unverständlich ist, dass die Europäische Union die bisher einzige internationale Konvention, nämlichdie UN-Konvention über den Abschluss elektronischer Verträge, nicht ratifiziert hat, obwohl die Union an der Ausarbeitung beteiligt war und diese Konvention eine Ergänzung zum Internationalen Kaufrecht (CISG) darstellt.[3]

1.1. E-Kommerz und Verantwortlichkeit der Vermittlungsdiensteanbieter

Die E-Commerce-Richtlinie[4] hat in Deutschland zur Änderung von fast einem Dutzend Gesetzen geführt, darunter insbesondere des Bürgerlichen Gesetzbuchs, des Telemediengesetzes und des Unterlassungsklagegesetzes. Das Verbraucherschutzrecht ist in Deutschland nicht (wie etwa in Österreich oder Polen) in einem Spezialgesetz geregelt. Das hat in der deutschen Gesetzgebung, Rechtsprechung und Praxis zu zahlreichen Problemen geführt.

Die meisten Vorschriften der E-Commerce-Richtlinie wurden aufgrund des „Gesetzes über rechtliche Rahmenbedinungen für den elektronischen Geschäftsverkehr (EGG)“[5] zunächst in das Teledienstegesetz (TDG) und in das Telekommunikationsgesetz (TKG), dann 2007 in das heutige Telemediengesetz (TMG) übernommen. Bei dem TKG steht die Transportleistung (Übertragung von Signalen), bei dem TMG der Inhalt der Informationen im Vordergrund.

Im TMG wurden die Verantwortlichkeiten der Diensteanbieter für eigene sowie für fremde gespeicherte, zwischengespeicherte („Caching“), durchgeleitete („Hosting“) Informationen präzisiert, Anbieterkennzeichnungen eingeführt und das Herkunftslandprinzip mit dem deutschen IPR in Einklang gebracht.

Frage 1.1.1.

In Deutschland war lange streitig, welche Dienstleister in den Genuss der Haftungsprivilegierungen der Art. 12-15 E-Commerce-Richtlinie kommen, auf die sich die §§ 7-10 TMG beziehen.Inzwischen besteht durch Hunderte von Gerichtsentscheidungen[6] und durch ausdrückliche gesetzliche Regelungen mehr Klarheit.

Durch Einfügung eines neuen 3. Absatzes in §10 TMG wurde im Juni 2016 klargestellt, dass eine zivil-, straf- oder verwaltungsrechtlicheHaftung von WLAN-Betreibern für Rechtsverletzungen ihrer Nutzer als sogenannte „Störer“ (also als mittelbar Verantworliche) nicht in Betracht kommt, soweit

[3] Boss/Kilian, The United Nations Convention on the Use of Electronic Communications in International Contracts. An In-Depth Guide and Sourcebook, Alphen aan den Rijn 2008.

[4] Richtlinie 2000/31/EG vom 8.6.2000 ABl. L 178 vom 17.7.2000, S. 1.

[5] BGBl. 2001, S. 3721.

[6] Die Datenbank https://dejure.org/gesetze/TMG weist zu § 8 TMG 131 Gerichtsentscheidungen nach, zu § 10 TMG insgesamt 224.

diese bestimmte Sorgfaltspflichten erfüllen. Gleichzeitig wurde geregelt, dass sich Host-Provider, deren Geschäftsmodell im Wesentlichen auf der Verletzung von Urheberrechten aufbaut, nicht auf das Haftungsprivileg berufen können.[7]

In Deutschland dürfte sichnach der Neuregelung die Haftungsprivilegierung der Access-Provider nach § 8 TMG nunmehr auch auf Unterlassungsansprüche erstrecken.[8] Dies hatte der Bundesgerichtshof bisher in ständiger Rechtsprechung verneint[9]. Der EuGH lässt Unterlassungsansprüche im Hinblick auf die Art. 12-15 der E-Commerce Richtlinie, die auf den §§ 8-10 TMG beruhen, dann zu, wenn gerichtliche Anordnungen vorliegen, die sich auf immaterialgüterrechtliche Ansprüche stützen.[10]

Umstritten ist noch, ob sich Betreiber von Suchmaschinen, Internet-Plattformen Videoportalen oder die Setzer von Hyperlinksauf die Privilegierung der §§ 8-10 TMG berufen können.[11]Als nicht ausdrücklich geregelt sieht der Deutsche Bundestag[12] auch die Voraussetzungen für Schadenersatzansprüche aus Persönlichkeitsrechtsverletzungen an, obwohl Art. 82 DSGVO und §83 BDSG 2017generell eine modifizierte Gefährdungshaftung des „Verantwortlichen" vorschreiben.

Im Übrigen meint der Deutsche Bundestag: „Ein einheitliches Haftungsregime für Rechtsverletzungen im Internet zu kodifizieren ist vorrangig eine europäische Aufgabe".[13]

Frage 1.1.2.

Die Untersuchung des EuGH im Fall L`Oréal SA[14] zu Verantwortlichkeiten eines Internet-Plattformbetreibers sind gründlich und nachvollziehbar. Heutesollteman allerdings überlegen, ob nach dem Stand der Technik der Einsatz von Filter- und Erkennungssoftware als Obliegenheit zumutbar ist, um rechtswidrige Angebote zu reduzieren.

Frage 1.1.3.

Das System „notice-and-take-down" eignet sich nicht, um allen Fällen von Beanstandungen gerecht zu werden, weil Beanstandungen auch unberechtigt sein

[7] BT-Drs. 18/6745 vom 1.6.2016.

[8] BT-Drs. 18/8645 vom 1.6.2016.

[9] BGH MMR 2007, 518; BGH MMR 2012, 124.

[10] EuGH vom 12.7.2011, C-324/09, L`Oréal SA, ECLI:EU:C:2011:474; EuGH vom 15.9.2016, C-484/14, McFadden, ECLI:EU:C:2016:689.

[11] Bejahend: OLG Köln, ZD 2017, 96; KG, MMR 2010, 495; ablehnend: Spindler/Schuster/Hoffmann, Recht der elektronischen Medien, 3.A. München 2015, § 8 TMG Rdnr. 24; LG Frankfurt, ZD 2017, 391.

[12] BT-Drs. 18/8645 vom 1.6.2016, 6.

[13] BT-Drs. 18/8645 vom 1.6.2016, S. 11.

[14] Urteil vom 12.7.2011, C-324/09, ECLI:EU:C:2011:474.

können oder Abwägungsprozesse erfordern. In krassen Fällen ist ein sofortiges „Take-down“ allerdings angemessen. Sinnvoll wäre es, im Hinblick auf Beanstandungen einen Maßnahmenkatalogzu entwickeln und bei den beanstandeten gespeicherten Inhalten jeweils darauf zu verweisen.

In Deutschland ist ein „Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken“[15] in Kraft getreten. Danach müssen große soziale Netzwerke – wie Facebook, Twitter oder YouTube –künftig Inhalte, die gegen 21 ausdrücklich aufgeführte Straftatbestände verstoßen, innerhalb von 24 Stunden löschen sowie nicht offensichtliche Verstöße innerhalb von sieben Tagen klären (§ 1). Das Prüfungsverfahren muss transparent und wirksam sein (§ 3). Bei systematischer Vernachlässigung dieser Verpflichtungen droht dem Netzwerkbetreiber ein Bußgeld von bis zu 5 Mio. Euro (§ 4 (2)).

Nach der gleichzeitig erfolgten Änderung des Telemediengesetzes darf der Diensteanbieter dem Verletzten nach gerichtlicher Anordnung Auskunft über vorhandene Bestandsdaten zur Durchsetzung zivilrechtlicher Ansprüche geben (§ 14 Abs. 3 und 4 TMG).

Soweit es um den Missbrauch personenbezogener Daten geht, ist unionsweit künftig auch das Widerspruchsrecht nach Art. 21 (5) DSGVO zu beachten.

Frage 1.1.4.

Bisher ist die Verwendung von Filtersystemen durch Internet-Dienstleister zur Abwehr urheberrechtlicher Verstöße unionsrechtlich nicht vorgeschrieben. Filtersystemewerden aber vom EuGH nicht verboten und sind von der Kommission geplant.[16]

Während einige Untergerichte in Deutschland Filtersysteme generell ablehnen[17], verlangt der Bundesgerichtshof „zumutbare Anstrengungen“[18] des Dienstleisters sowie Nachforschungen des Rechteinhabers, die zu gerichtlich angeordneten Sperrmaßnahmen gegen bestimmte Kunden führen können. Bei allen Maßnahmen sind verschiedene Grundrechte (Telekommunikationsgeheimnis; Datenschutz; Eigentumsgarantie; Meinungsäußerungsfreiheit; Urheberrecht) gegeneinander abzuwägen. Die Beweislast dafür, dass zumutbare Maßnahmen getroffen wurden, trägtder Internet-Dienstleister.[19]

[15] Netzwerkdurchsetzungsgesetz (NetzDG) vom 1.9.2017, BGBl. I S. 3352.

[16] Art. 13 des Vorschlags für eine Richtlinie über das Urheberrecht im Binnenmarkt, COM(2016) 593 final.

[17] OLG Hamburg, 21.11.2013, 5 U 68/10

[18] BGH GRUR 2008, 702.

[19] BGH openJur 2016,235.

1.2. Verbraucherschutz in Bezug auf das Internet und den E-Kommerz

Der Verbraucherschutz (B2C-Verträge) spielt bei elektronischen Verträgen deshalb eine große Rolle, weil bei elektronischen Verträgen auf der gleichen Stufe (B2B; C2C) grundsätzlich von gleichem Informationsstand und gleicher Verhandlungsmacht der Beteiligten ausgegangen werden kann. Eine Informationsassymmetrie[20]wird hypothetisch nur bei B2C-Verträgen im Internet angenommen.

Frage 1.2.1.

Die zwingenden Vorschriften der Verbrauchsgüterrichtlinie mussten mit dem grundsätzlich dispositiven Zivilrecht innerhalb des BGB in Einklang gebracht werden. Das Grundmodell des Vertrages (Angebot und Annahme) ist weiterhin gültig, jedoch mussten viele Modalitäten des Vertragsabschlusses(Authen tizität; Identifizierung; Liste der Informationspflichten; Webseite als Antrag oder invitatio ad offerendum; E-Mail-Vertragsschluss; Internet-Versteigerungen; Widerrufsvoraussetzungen) geklärt und in das Rechtssystem integriert werden.

Frage 1.2.2.

Hindernisse im Online-Handel sind durch die von der Kommission veranlassten empirische Untersuchungen der Kommission gut belegt.[21]Erheblich vernachlässigt wird allerdings die Tatsache der Sprachbarrieren.

Für den Versuch, personenbezogene Daten als „Gegenleistung anders als Geld" zu klassifizieren, fehlt dierechtsdogmatische Fundierung.Implizit wird der „Geldwert" personenbezogener Daten als eigentumsähnliches Recht anerkannt.

Die Abgrenzung zwischen „aktiver" und „passiver" Zurverfügungstellung von personenbezogenen Daten ist undurchführbar, weil beispielsweise die Möglichkeit nachträglicherprofitabler Sekundärauswertungen der „Gegenleistung" nicht reflektiert wird.Wie hoch ist der Wert der „Gegenleistung"?

Frage 1.2.3.

Die Richtlinienvorschläge 634 und 635 sollten zusammengefasst werden. Die Differenzierung zwischen Online- und Offline- Verkäufen ist bei Sachgütern nicht überzeugend. Beide Verfahren unterscheiden sich nur durch das Verfahren des Vertragsabschlusses, nicht aber durch die Vertragsabwicklung (physische Übergabe; Nachprüfungsmöglichkeiten).

[20] Fleischer, Informationsassymmetrie und Vertragsrecht, München 2001.
[21] COM (2015) 635 final, Fußnote 31.

Frage 1.2.4.
Eine „Vollharmonisierung" kann allenfalls langfristig durch die Auslegung des EuGH gelingen.

Frage 1.2.5.
Die bestehenden Richtlinien sind grundsätzlich ausreichend und bedürfen lediglich punktueller Ergänzungen.

Frage 1.2.6.
Es gibt zahlreiche Verfahren gegen Vertragsklauseln von Online-Diensteanbietern in Deutschland.[22] In jüngerer Zeit haben deutsche Verbraucherschutzverbände mehrere Verfahren gegen Vertragsklauseln von Facebook eingeleitet[23], weil deren AGB dem deutschen (und europäischen) Datenschutzrecht teilweise widersprechen. Facebook bietet neuerdings besondere AGB für Nutzer in Deutschland an, die sich von ihren AGB in anderen Staaten unterscheiden.

Frage 1.2.7.
Eine Ausweitung der geplanten Vorschriften für den Online-Handel zwischen Unternehmen (B2B) wäre systemwidrig. Zwischen Unternehmen wird der gleiche Informationsstand und die gleiche Verhandlungsmacht unterstellt, so dass keine Schutzbedürftigkeit angenommen werden kann.

1.3. Geoblocking

„Geoblocking" wird in dem Vorschlag COM (2016) 289 verkürzt unter dem Gesichtspunkt der Diskriminierung gesehen. Unterschiedliche Geschäftsbedingungen sind aber aus Wettbewerbsgründen nach primärem Unionsrecht nur dann unzulässig, wenn der Missbrauch einer marktbeherrschenden Stellung (Art. 102 AEUV) vorliegt. Wenn funktionsfähiger Wettbewerb herrscht, bestehen für einen Verbraucher Auswahlmöglichkeiten, solangeTransparenz über die Angebote herrscht.

[22] BGH K&R 2006, 460: Verlinkte AGB müssen einsehbar und ausdruckbar sein; LG Berlin, K&R 2014, 544: Messenger-Dienst „WhatsApp" muss AGB in deutscher Sprache anbieten; BGH MDR 2010, 677: Klauseln über unterschiedliche Gebühren bei Flugbuchungen sind unzulässig; OLG Dresden K&R 2015, 262: Es muss mindestens eine gängige unentgeltliche Zahlungsmöglichkeit angeboten werden; BGH K&R 2016, 505: Eine Kontaktaufnahme nur gegen Entgelt ist unzulässig;OLG Frankfurt CR 2006, 195: Eine Klausel, dass die Lieferung nur unter Vorbehalt erfolge, ist unzulässig; LG Berlin K&R 2012, 300: Kontaktaufnahme ohne vorherige Einwilligung ist unzulässig.

[23] Anhängige Verfahren:Beim LG Berlin 16 O 341/15 (Irreführung durch Aussage „Facebook ist und bleibt kostenlos"); beim BGH I ZR 65/14 (unzulässige Anwendung des kalifornischen Rechts statt des deutschen (und europäischen) Datenschutzrechts).

Das Wohnortprinzip als Anknüpfung für Klagen des Verbrauchers oder gegen den Verbraucher nach der Verordnung 1215/2012[24] wird in COM (2016) 289 beibehalten.[25]Der Hinweis in Erwägungsgrund 10 (2. Satz) der geplanten Verordnung ist überflüssig, scheint aber die Notwendigkeit der Anknüpfungsgesichtspunkteder geplanten Verordnung legitimieren zu sollen.

1.4. Fragen in Bezug auf die kollaborative Wirtschaft

Die Agenda COM (2016)356 unterscheidet leider nicht konsequent zwischen der Organisationeiner elektronischen Plattform, deren Betreibersowie derPlattformnutzung durch Dritte.

Frage 1.4.1.

Der Bundesgerichtshof hat dem EuGH im Hinblick auf den Fahrdienst-Vermittler „Uber" die Frage vorgelegt, ob Uber Mietwagen mit Fahrer per Smartphone-App direkt vermitteln darf, ohne auf feste Tarife wie bei Taxis verpflichtet zu sein.[26]

Die Stadt Freiburg darf von einem Online-Buchungsportal, über das private Zimmer- und Wohnungen angemietet werden können, Auskünfte zum Zweck der Berechnung der örtlichen Übernachtungssteuer verlangen.[27]

Ein Online-Lieferdienst haftet für Wettbewerbsverstöße als Täter.[28]

Frage 1.4.2.

Wettbewerbsprobleme bestehen dann, wenn gewerblich über elektronische Plattformen betriebene Peer-to-Peer Tätigkeiten nicht denselben Bedingungen (z.B. Versicherungspflichten; Haftung) wie traditionelle Dienstleister unterliegen. Diskrepanzen könnten durch Anwendung der Richtlinie 2013/55/EU[29]gewerbliche Anbieter beseitigt werden.

Frage 1.4.3.

Genehmigungen sind nur im Bereich der regulierten Berufe erforderlich.Sie hängen von beruflichen Qualifikationsvoraussetzungen ab, die im öffentlichen Interesse erlassen worden sind.

[24] Eine Verordnung 1215/2015 (Fragebogen S. 8, 1.Zeile) gibt es nicht.
[25] Erwägungsgrund 10.
[26] Beschluss vom 18.5.2017, Az. I ZR 3/16.
[27] Urteil vom 5.4.2017 (www.vgfreiburg.de/pb/Lde/4609571/?LISTPAGE=1215608), besucht m11.9.2017).
[28] KG vom 21.6.2017, % U 185/16 (www.online-und-recht.de), besucht am 11.9.2017).
[29] ABl. L 345 vom 28.12.2013, S. 132.

Frage 1.4.4.
Für Verbraucher wurde die Möglichkeit eröffnet, Schiedsvereinbarungen elektronisch abzuschließen (§ 1031 Abs. 5 S. 2 ZPO).

Frage 1.4.5.
Die Klassifikation als „gewerblicher" Diensteanbieter hängt von der Häufigkeit und dem Umfang der Transaktionen ab. Das wird durch Handels- und Steuerrecht geklärt.

Frage 1.4.6.
Gütezeichen einer anerkannten neutralen Organisation sind ein gutes Mittel zur Schaffung von Transparenz. Im Übrigen sind Verbandsklagen zur Kontrolle der AGB von Plattformbetreibern sinnvoll.

2. Digitale Media

Frage 2.1.
Dem Berichterstatter liegen keine konkreten Erkenntnisse dazu vor. Es ist allerdings anzumerken, dass deutsche Behörden aufgrund des Legalitätsprinzips verpflichtet sind, stets nach dem geltenden Recht zu handeln, wozu auch die Vorgaben des Unionsrechts gehören, wobei ihnen allerdings in gewissen Grenzen ein Aufgreifermessen zusteht.

Das EuGH-Urteil hat der Konvergenzdiskussion neuen Auftrieb gegeben. In Anmerkungen zu dem Verfahren wird daraus die Notwendigkeit abgeleitet, die analog geprägte Begriffswelt der AVMD-Richtlinieanan die Besonderheiten der modernen Kommunikationsinstrumente anzupassen.[30]Es sei zudem ein grundsätzliches Dilemma, dass der Übergang schleichend sei zwischen den klassischen Massenmedien mit entsprechender Bedeutung für die Meinungsbildung, hybriden Inhalten, wie sie die Informationsportale darstellen, und rein privaten Inhalten, wie etwa auf Youtube oder Facebook, weil auch letztere potenziell ungeahnte Massen erreichen könnten.[31]Darüber hinaus wurde betont, dass die inhaltliche Medienregulierung nicht der Union obliege, sondern den Mitgliedstaaten.[32]

[30] *Nikolaus Peifer*, Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht (GRUR-Prax) 2015, S. 327 (zu den Schlussanträgen des Generalanwalts).
[31] *GeraldSpindler*, Juristenzeitung 2016, S. 147, 149.
[32] *Nikolaus Peifer*, Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht (GRUR-Prax) 2015, S. 327 (zu den Schlussanträgen des Generalanwalts).

2.2.

Der Frage zur Einbindung von Video-Plattformen in den Anwendungsbereich der AVMD-Richtlinie liegt ein so komplexes Interessengeflecht zugrunde, dass sich einfache Antworten verbieten. Zunächst muss zur Kenntnis genommen werden, dass sich der Medienkonsum in Deutschland stark von den linearen hin zu den nicht-linearen Medien entwickelt.[33] 65,1 % der deutschen Bevölkerung, also 45,1 Millionen Personen, nutzen täglich das Internet. Im Jahr 2016 nutzten 72% der Bevölkerung ab 14 Jahren zumindest gelegentlich das Internet für den Konsum von Videos. Dieser Wert lag im Jahr 2011 noch bei 50%. Betrachtet man die Altersstruktur der Nutzer, fällt auf, dass besonders viele Menschen im Alter von 14 bis 29 Jahren die Videonutzung im Internet in Anspruch nehmen: 43% im Alter von 14 bis 29 Jahren nutzten Videostreamingdienste.

Auf der einen Seite ist daher die Notwendigkeit hervorzuheben, ein *level playing field* für Anbieter zu schaffen, die um dieselben Zielgruppen konkurrieren und von denen dieselben regulationswürdigen Risiken ausgehen. Schon die existierende Richtlinie betontdie Grundsätze des freien Wettbewerbs und der Gleichbehandlung sowie die Notwendigkeit,Wettbewerbsverzerrungen zu vermeiden(Erwägungsgründe 10 und 11 RL 2010/13/EU). Zudem ist es Aufgabe der Union, neben der kulturellen Vielfalt ein hohes Schutzniveau beim Jugend- und Verbraucherschutz zu gewährleisten(Erwägungsgründe 12 RL 2010/13/EU).

Auf der anderen Seite darf der Pluralismus der Medienformate nicht durch eine übermäßige Regulierung verhindert werden. Gerade im Internet bieten viele kleine, neu gegründete Unternehmen Dienste an, so dass eine mehr als die „absolut erforderliche Regulierung" (Erwägungsgrund 14 RL 2010/13/EU) abschreckende Wirkung und eine Senkung der Pluralität zur Folge haben kann. Zudem muss bedacht werden, dass ein zentraler, behördlicher Regulierungsansatz bei einigen wenigen großen Anbietern erfolgsversprechend ist, ein solcher Ansatz aber bei der Regulierung einer fast unüberschaubar großen Anzahl kleiner Anbieter schnell an seine systemimmanenten Grenzen stoßen kann. Darüber hinaus können die Regulierungskonzepte eines linearen Mediums nicht ohne Weiteres auf nicht-lineare Angebote übertragen werden. Ferner muss auch auf die Akzeptanz der Regulierung auf der Nutzerseite geachtet werden. So ist etwa durch Gewöhnung weitgehend akzeptiert, dass aus Gründen des Jugendschutzes gewisse Arten von Sendungen erst ab einer bestimmten Uhrzeit ausgestrahlt werden dürfen. Dieselbe Regulierung von Internetdiensten stößt dagegen auf wenig Verständnis und wirkt gekünstelt, wenn etwa bestimmte Krimisendungen wie solche der Tatort-Reihein der Mediathek des Senders erst ab einer bestim-

[33] Zu den folgenden Zahlen ARD/ZDF-Onlinestudie 2016,*Wolfgang Koch/BeateFrees,* Media Perspektiven 2016, S. 418-437 und *Thomas Kupferschmitt*, Media Perspektiven 2016, S. 448-459.

mten Uhrzeit zum Abruf bereitstehen dürfen, aber gleichzeitig viel intensivere Gewaltszenen nur wenige Klicks entfernt rund um die Uhr zugänglich sind. Es steht daher zu befürchten, dass Nutzer auf vollständig unregulierte Angebote ausweichen, was den Zielen der Regulierung abträglich wäre.

Dementsprechend ist der grundsätzliche Ansatz zu begrüßen, auch Video-Plattformen in den Anwendungsbereich der Richtlinie aufzunehmen. Es sollte allerdings ein medienspezifischer Regulierungsansatz verfolgt werden, der den Besonderheiten der verwendeten Medienund der unterschiedlichen Anbietersowie Nutzerstruktur Rechnung trägt.

Moderne Werbeformen sind ein wichtiges Finanzierungsmittel audiovisueller Mediendienste. Dennoch ist es für die Meinungsbildung unerlässlich, dass Konsumenten zwischen werblicher Kommunikation und redaktionellen Inhalten unterscheiden können. Für sie sollte daher medienübergreifend unmittelbar erkennbar sein, ob sie sich in einem kommerziellen oder redaktionellen Umfeld befinden. Die konkrete Ausgestaltung der Kennzeichnung sollte wiederum medienspezifisch angepasst und den Besonderheiten des Mediums und der jeweiligen Zielgruppe Rechnung tragen.

Darüber hinaus muss auch hier ein *level playing field* zu den traditionellen Anbietern audio-visueller Dienste sichergestellt werden. Es sollte daher medienübergreifend ein Gleichgewicht zwischen dem Verbraucherschutz und der Wettbewerbsfähigkeit hergestellt werden. Welche Regulierungsinstrumente hierfür eingesetzt und wie diese mit anderen Instrumenten, etwa dem Lauterkeitsrecht, abgestimmt werden, bedarf aber der vertieften Diskussion.

In Deutschland unterliegen solche audiovisuellen Plattformen den für Telemedien geltenden Bestimmungen des TMG[34], dessen Regelungen die AVDM-RL nicht 1:1 umsetzen, an dessen Zielrichtung sie aber orientiert sind.[35] Die audiovisuellen Mediendienste sind in § 2 S. 1 Nr. 6 TMG legaldefiniert. Danach sind „audiovisuelle Mediendienste auf Abruf" Telemedien mit Inhalten, die nach Form und Inhalt fernsehähnlich sind und die von einem Diensteanbieter zum individuellen Abruf zu einem vom Nutzer gewählten Zeitpunkt und aus einem vom Diensteanbieter festgelegten Inhaltekatalog bereitgestellt werden. Das TMG trifft in §§ 2 S. 1 Nr. 1 Hs. 2, § 2 a II-IV TMG Sonderregelungen für „audiovisuelle Mediendienste auf Abruf" und enthält in § 1 Abs. 6 TMG eine Bereichsausnahme für solche Dienste, die ausschließlich zum Empfang in Drittländern bestimmt sind undnicht unmittelbar oder mittelbar von der Allgemeinheit mit handelsüblichen Verbraucherendgeräten empfangen werden können.

[34] Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Art. 1 G v. 21. Juli 2016 (BGBl I 1766).

[35] Vgl. Bundestagsdrucksache 17/718, S. 8.

Frage 2.3.
Dem Berichterstatter sind solche Streitigkeiten nicht bekannt und es wird über solche Streitigkeiten auch nicht in der einschlägigen Literatur berichtet. Vielmehr wird konstatiert, dass der kontroversen rechtspolitischen Diskussion keine entsprechende (veröffentlichte) Behörden- und Gerichtspraxis nachfolgte, wobei nicht auszuschließen ist, dass sich dies ändern kann.

Dem Berichterstatter sind solche Streitigkeiten nicht bekannt und es wird über solche Streitigkeiten auch nicht in der einschlägigen Literatur berichtet.

Frage 2.4.
Es ist ein grundsätzlich sehr unterstützungswürdiges Anliegen, Unabhängigkeitsanforderungen für die Medien-Regulierungsbehörden zu formulieren. Allerdings erscheint es sinnvoll, in erster Linie qualitative Anforderungen an die Zusammensetzung und Unabhängigkeit der Gremien zu stellen und die Organisationsform weiter den Mitgliedstaaten zu überlassen.

Der Effekt unabhängiger Medien-Regulierungsbehörden auf den freien Binnenmarkt erscheint nur sehr schwer quantifizierbar.

In Deutschland ist das Gebot der Staatsferne des Rundfunks verfassungsrechtlich verankert. Die Unabhängigkeit und Weisungsfreiheit der Landesmedienanstalten, den Aufsichtsbehörden des privaten Rundfunks, wird von den einzelnen Landesmediengesetzen gewährleistet. Die Aufsichtsgremien der öffentlich-rechtlichen Rundfunkanstalten haben ihre Rechtsgrundlage in Rundfunkgesetzenund in den durch Gesetze umgesetzten Staatsverträgen der Länder. Versuche der Politik, zu starken Einfluss in den Aufsichtsgremien zu erhalten, können vor dem Bundesverfassungsgericht angegriffen und überprüft werden, wie zuletzt mit dem Normenkontrollantragdes ZDF-Staatsvertrag vom 25. März 2014 (Az. 1 BvF 1/11 und 4/11).Danach ist der Einfluss der staatlichen und staatsnahen Mitglieder in den Aufsichtsgremien konsequent zu begrenzen.Der Anteil der staatlichen und staatsnahen Mitglieder darf insgesamt ein Drittel der gesetzlichen Mitglieder des jeweiligen Gremiums nicht übersteigen. Zudem dürfen Vertreter der Exekutive keinen bestimmenden Einfluss auf die Auswahl der staatsfernen Mitglieder haben.

Frage 2.5.
Es kann von zwei Fällen berichtet werden, die sowohl die Öffentlichkeit als auch Gerichte beschäftigt haben: Der Dschungelcamp-Fall stand aufgrund der Bekanntheit der Sendung besonders im Fokus der Öffentlichkeit.[36] Elf mehr oder weniger bekannte Kandidaten mussten für die Sendung in einem Camp

[36] Verwaltungsgericht Hannover, Urteil vom 18. Februar 2016 – 7 A 13293/14 = AfP 2016, 378.

im australischen Urwald leben und wurden dort auf eine karge Diät gesetzt. Sie konnten sich durch Mutproben u.a. eine Schatzkiste erspielen, in der die Produktionsfirma eine Packung Kekse der Marke „Leibniz Pick Up" platziert hatte. Nach Öffnung der Kiste folgten zwei Minuten Sendezeit, in denen auf verschiedenste Weise für das Produkt geworben wurde. Unter anderem wurden die Vorzüge des Produkts durch technische Nachbearbeitung sowie die Lobpreisungen der Teilnehmer in den Interviews, aber auch durch das genüssliche Stöhnen beim Verzehr des Produkts verstärkt. Ferner wurde häufig die Verpackung des Produkts durch Slow-Motion Elemente und anderweitige Effekte in Szene gesetzt.

Im anschließenden medien-aufsichtsrechtlichen Verfahren wurde über die Frage gestritten, ob die Darstellung des Produkts „zu stark" im Sinne des § 7 Abs. 7 Satz 1 Nr. 3 RStV[37] war. Das angerufene Verwaltungsgericht Hannover ging aufgrund der vorgehend beschriebenen Darstellungen des Produkts davon aus, dass der Werbezweck das Geschehen in der Sendung dominiert hatte.

In einem anderen Fall beanstandete die Kommission für Jugendmedienschutz (KJM) eine Beeinträchtigung der Jugend durch die Ausstrahlung einer Folge der Serie „Sex and the City" („Heimlicher Sex").[38]Nach Ansicht der KJM verstieß die Ausstrahlung der Folge im Tagesprogramm gegen § 5 Abs. 4 Satz 3 i. V. m. Abs. 1, 2 JMStV[39]. Es sei eine „sexualethische Desorientierung von Kindern unter 12 Jahren zu befürchten", da Kinder teilweise die ironisch gemeinten Darstellungen der Serienrollen missverstehen könnten. § 5 Abs. 1 JMStV erfasst Sendungen, „die geeignet sind, die Entwicklungen von Kindern oder Jugendlichen zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit zu beeinträchtigen". Das vom Sender angerufene Verwaltungsgericht Berlinfolgte der Auffassung der KJM, dass die sprachliche Gestaltung der Sendung der gesellschaftlichen Wertvorstellung der Bundesrepublik hinsichtlich der Entwicklung und der sittlichen Erziehung widerspreche. Das Gericht war der Ansicht, dass der Kläger seiner Pflicht aus § 5 Abs. 1 JMStV durch die Anpassung der Sendezeit nachkommen könne.

Der Reformvorschlagder EU-Kommission berücksichtigt eine große Bandbreite an Themen, deren Implementierung abgewartet und ihre Auswirkungen evaluiert werden sollten, bevor ein weiterer Reformbedarf angegangen werden sollte.

[37] Staatsvertrag für Rundfunk und Telemedien, in der Fassung vom 09. September 2015.

[38] Verwaltungsgericht Berlin, Urteilvom 09. November 2011 – 27 A 64.07 = ZUM 2012, 417.

[39] Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien, vom 13. September 2002.

Frage 2.6.

Das Thema *adressable TV,* also personalisierte Fernsehwerbung, wird von den privaten Fernsehanstalten als Trend-Thema hervorgehoben.[40]Besitzt der Zuschauer ein Smart TV mit Internetanschluss, wird beim Umschalten auf ein neues Programm eine Art digitaler Banner auf das laufende Programm gelegt. Auf diese Weise bietet etwa die TV-Gruppe ProSiebenSat.1 ihren Werbekunden die Möglichkeit an, die Werbung nach Kategorien wie Regionen oder Wetterverhältnissen zu differenzieren, so dass ein anderes Werbemittel in Regionen mit Sonnenschein wird als in Regionen, in denen das Wetter gerade schlechter ist. Darüber hinaus bietetsie die Möglichkeit, nach AGF-Daten zu selektieren, also etwa Haushalte mit Kindern, Einzelhaushalte, etc.

Voraussetzung für die Werbeform ist aber, dass die Zuschauer ein Smart TV verwenden, das mit dem Internet verbunden ist. Diese Voraussetzung erfüllen derzeit rund zehn Millionen Geräte in Deutschland. Das Werbeformat spielt jedoch bislang nur eine Nebenrolle. So hat ProSiebenSat.1 im Jahr 2016 nach eigenen Angaben rund 100 *adressable TV* Kampagnen ausgespielt und dabei einen kleinen einstelligen Millionenbetrag umgesetzt.

Wenn ja, wie geschah das im Licht der Sendungs/Datenschutzrechtsnormen? Gab es eine Art von Kooperation zwischen der Medien-Regulierungsbehörde und der Datenschutzbehörde?

Dazu sind keine Informationen verfügbar.

Glauben Sie, dass eine europaweit harmonisierte Annäherung hier angebracht wäre?

Europaweit harmonisierte Regeln wären sinnvoll, insbesondere um die Regeln mit dem Datenschutzrecht in Einklang zu bringen, das in der Datenschutz-Grundverordnung 2016/679 harmonisiert ist.

Frage 2.7.

Die Richtlinie 93/83 EWG wurde in Deutschland in den §§ 20a und 20b UrhG[41] umgesetzt. Diese sind weiter in Kraft.

Das Recht der europäischen Satellitensendung (§ 20a UrhG) findet aufgrund seiner technischen Definition keine Anwendung auf die digitale Distribution urheberrechtlich geschützter Werke über das Internet und andere netzvermittelte Abrufdienste.[42] Darüber hinaus ist es in Deutschland umstritten, inwieweit Online-Übertragungen von Sendungen dem Senderecht (§ 20 UrhG) oder dem Recht auf öffentliche Zugänglichmachung (§ 19a UrhG) unterfallen sollen. Es

[40] Vgl. hierzu und zum Folgenden http://meedia.de/2017/06/06/personalisierte-tv-werbung-bei-prosiebensat-1-wir-haben-gar-nicht-vor-klassische-werbebloecke-gegen-adressable-tv-zu-tauschen/

[41] Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), zuletzt geändert durch Artikel 1 des Gesetzes vom 1. September 2017 (BGBl. I S. 3346).

[42] *Dustmann*, in: Fromm/Nordemann, UrhG, 11. Auflage 2014, § 20a Rn. 7 mwN.

zeichnet sich aber eine Differenzierung ab, wonach Streams, die das gesendete Programm begleitend und zu festen Zeiten abbilden (Live-Streaming/Webcasting/Simulcasting/Near-onDemand), als Sendung nach § 20 UrhG qualifiziert werden,und zeitversetzte On-Demand-Streams, die an keine feste Abfolge gebunden sind, als öffentliche Zugänglichmachung (§ 19a UrhG) eingeordnet werden.[43]

Frage 2.8.
(Lizenz-)Vertragliche Restriktionenwaren die hauptsächliche Hürde für die Portabilität digitaler Inhalte. Nach In-Kraft-Treten der VO (EU) 2017/1128 vom 14. Juni 2017 zur grenzüberschreitenden Portabilität von Online-Inhaltediensten im Binnenmarkt sind diese Hürden im Anwendungsbereich der Richtlinie abgebaut worden.

Die Vorgaben in Art. 5 VO (EU) 2017/1128, wonach der Anbieter den Wohnsitzmitgliedstaat des Abonnenten nur bei Abschluss und Verlängerung eines Vertrags sowie bei begründeten Zweifeln am Wohnsitzmitgliedstaat überprüft, scheint ein angemessener Kompromiss zwischen den Interessen der Anbieter und der Nutzer darzustellen.

3. Digitale Infrastrukturen

Die digitalen Infrastrukturen legen die technischen Voraussetzungen für die Möglichkeiten der elektronischen Kommunikation fest. In einer Erklärung der EU-Kommission, die der Richtlinie 2009/40/EG[44] beigefügt war, wurde die Wahrung der „Netzneutralität" zum politischen Ziel erhoben. Die ursprüngliche Idee der Netzneutralität bestand darin, für alle Nutzer eine gleichberechtigte „end-to-end" Verbindung im Internet zu garantieren.[45] Dieses Konzept wurde jedoch nicht verwirklicht. Das Wort „Netzneutralität" taucht in der Verordnung (EU) 2015/2120 auch nicht mehr auf. Stattdessen geht es um den diskriminierungsfreien Zugang zum Internet, um Wettbewerb, Technologieneutralität, Verbraucherschutz und Datenschutz. Unter den Stichwörtern „Qualität der Dienste", „spezielle Verkehrskategorien" und „Verkehrsmanagement" verbirgt sich die Möglichkeit, auf der Grundlage von Breitbandnetzen und des neuen Internetprotokolls IPv6 bestimmte Nutzer gegen Extrazahlungen (z.B. Übermittlung von Bankdaten) zu bevorzugen.Garantiert wird lediglich einleistungsmäßig nicht näher definierterInternetzugang für alle.

[43] *Ehrhardt*, in: Wandtke/Bullinger,Praxiskommentar zum Urheberrecht, 4. Auflage 2014, § 20 Rn. 4; *Dustmann*, in: Fromm/Nordemann, UrhG, 11. Auflage 2014, § 19a Rn. 25 mwN.
[44] ABl. L 337 vom 18.12.2009, S. 37.
[45] Van Schewick, Internet Architecture and Innovation, M.I.T Press 2010.

Frage 3.1.
In Deutschland wurde im Jahre 2012 ein § 41a in das TKG zur Netzneutralität in Form einer Verordnungsermächtigung für die Regierung und für Anordnungen der Bundesnetzagentur eingeführt. Eine Regierungsverordnung wurde nicht verabschiedet. Die Bundesnetzagentur ging gegen die Deutsche Telekom wegen Verletzung der Netzneutralität (Volumenbegrenzung; „managed services") vorund hielt das „zero rating" für eine Verletzung der Netzneutralität.[46] Inhaltliche Konkretisierungen der Netzneutralität blieben aber strittig.

Der 41a TKG wurde aufgrund der Verordnung 2015/2120 für überholt angesehen und deshalb im Jahre 2017 gestrichen.[47]Die EU-Verordnung lässt nun Geschäftsmodelle auf der Grundlage verschiedener Datenvolumina, Geschwindigkeiten und Qualitätsmerkmale unter bestimmten Bedingungen zu.

Die Bundesnetzagentur hat mehrere Verfahren wegen Zero-Rating Angebote durchgeführt und 2016/2017 zwei Angebote der Deutschen Telekom kritisch geprüft. Daraufhin hat die Deutsche Telekom eines der Angebote für Neukunden eingestellt. Ihr anderes Angebot „Stream On" ist seit dem 19.4.2017 auf dem Markt und steht noch unter Beobachtung der Bundesnetzagentur.[48]

Frage 3.2.
Ein europaweites Lizensierungssystem erscheint überflüssig, wenn Wettbewerb in der Breitbandkommunikation herrscht. Dafür ist aber der Ausbau der Breitbandnetze Voraussetzung. Deutschland lag im 1. Quartal 2017 mit durchschnittlich 15,3 Mbit/s Internetzugangsgeschwindigkeit weltweit an 25. Stelle (Schweden 23,5 Mbit/s an 3. Stelle). Die Bundesregierung wollte ursprünglich mit einem Technologiemix bis 2018 für alle Haushalte 50 Mbit/s im Downstream erreichen, während die Bundesländer stets die vollständige Umstellung auf Glasfaser bevorzugten.[49] Inzwischen unterstützt die Bundesregierung marktgetrieben („Industrie 4.0") und wohl auch aufgrund von Bedenken der EU-Kommission gegen einen Technologiemix die Umstellung auf Glasfaser. Sie will bis 2023 dafür 100 Mrd. Euro für Glasfasernetze zur Verfügung stellen.[50]Es wurden Förderrichtlinien und Verwaltungsvorschriften erlassen undbereits erhebliche staatliche Zuwendungen auf dieser Grundlage gewährt.

[46] Bericht der Bundesnetzagentur vom 14.6.2013 zur Tarifänderung der Deutschen Telekom AG für Internetzugänge (www.bundesnetzagentur.de/netzneutralität, besucht am 10.9.2017)
[47] 3. TKG-Änderungsgesetz vom 27.6.2017, BGBl. I S. 1963.
[48] Netzneutralität in Deutschland. Jahresbericht 2016/2017 der Bundesnetzagentur, S. 9 (https://www.bundesnetzagentur.de), besucht am 22.9.2017.
[49] Beckert, Ausbaustrategien für Breitbandnetze für Europa, Gütersloh (Bertelsmann-Stiftung) 2017, S. 63 (www.
[50] Handelsblatt vom 28.6.2017.

Frage 3.3.
Es bestehen wettbewerbsrechtliche Probleme im Hinblick auf das Verfahren VDSL2-Vectoring, das die Deutsche Telekom als früherer Monopolist für ihre veralteten Kupferleitungen anwendet, um Datenübertragungsraten von bis zu 100 Mbit/s im Downstream zu erzielen. Konkurrenten möchten die Deutsche Telekom zur teuren Umstellung auf Glasfaser zwingen, um über die Anmietung dieser Leitungen Zugang zu Endkunden zu gewinnen (Kampf um „die letzte Meile"). In einigen deutschen Städten gibt es Glasfasernetze, die von kleineren Konkurrenten der Deutschen Telekom betrieben werden.

Bei der Bundesnetzagentur ist zahlreichen Beschwerden (Preisgestaltung; Volumenbeschränkungen; Zeitbegrenzungen) nachgegangen und hat große Internetdienstleister überprüft, Geschwindigkeitsparameter konkretisiert und einen Qualitätsüberwachungsmechanismus entwickelt.[51] In Deutschland ist am 1.6.2017 eine Verordnung zur Förderung der Transparenz auf dem Telekommunikationsmarkt[52] in Kraft getreten, die im Vergleich zur VO (EU) 2015/2110 zusätzliche Anforderungen enthält (etwa über: Inhalte von Produktinformationsblättern; minimale und maximale Übertragungsraten; effektive Kostenkontrolle).

Frage 3.4.
Die Unabhängigkeit der nationalen Regulierungsbehörde (Bundesnetzagentur), die als selbständige Bundesoberbehörde organisiert ist,[53]wurde nie bestritten.

4. Daten in der digitalen Wirtschaft

Durch die digitale Erfassung von Sprache, Musik, Bildern, Verhaltensweisen, Zuständen, Abläufen oder Relationen entstehen Hierarchien von Daten, die unter den Bedingungen der elektronischen Datenverarbeitung grundsätzlich für viele Zwecke genutzt werden können. Wenn diese Daten durch Programme gespeichert, selektiert, kombiniert und zweckbezogen ausgewertet werden, können daraus wirtschaftlich verwertbare Informationen und neue Geschäftsmodelle entstehen. Da die Nutzungsmöglichkeiten für Daten nicht voraussehbar sind, ist in Deutschland eine heftige Auseinandersetzung darüber entbrannt, ob Daten grundsätzlich frei zugänglich sein sollten, um innovative Lösungen zu erleichtern, oder ob proprietäre Rechte daran bestehen oder ob solche Rechteneu geschaffen werden sollten.

[51] Netzneutralität in Deutschland. Jahresbericht 2016/2017 der Bundesnetzagentur (https://bundesnetzagentur.de), besucht am 28.8.2017.
[52] TKTransparenzV vom 19.12.2016 BGBl. I S. 2977.
[53] Bundesnetzagenturgesetz (BNetzAG) vom 7.7.2005, BGBl. I S. 1970.

Diese Diskussion wird in Deutschland sowohl unter Ökonomen[54] als auch unter Juristen[55] geführt. Dabei wird allerdings oft der informationstheoretische Unterschied zwischen „Daten" als bloße Nachrichten und „Informationen" als zweckbezogene Nachrichten vernachlässigt. Eine Differenzierung könnte aber interessante Ansatzpunkte für juristische Lösungen bieten. Deutsche Juristen neigen dazu, die Bezeichnungen „Daten" und „Informationen" synonym zu verwenden.Gleiches gilt für den deutschen und den europäischen Gesetzgeber. Beim „Datenschutz" geht es beispielsweise in erster Linie um den Schutz personenbezogener Informationen.

Aus ökonomischer Sicht können Informationen/Daten entweder als öffentliche Güter (public goods) angesehen werden, die frei zugänglich sind, oder als private Güter, an denen eigentumsähnliche Rechte (property rights) bestehen. Als Abrenzungskriterium dient der Aspekt, ob es möglich ist, Dritte von der Nutzung auszuschließen.Davon hängt die Vermarktbarkeit eines Gutes ab, denn niemand wäre bereit, ein Gut zu erwerben, das auch kostenlos genutzt werden kann.

Juristisch hängt die Ausschließungsmöglichkeit Dritter an der Nutzung eines Guts von der Zuerkennung von Eigentum oder eines eigentumsähnlichen Rechts an dem Gut ab.Die Möglichkeit, „Eigentum" an Daten erlangen zu können, wird zutreffend fast einhellig mit der Begründung abgelehnt, dass sich „Eigentum" in der Tradition des Römischen Rechts nur auf körperliche Gegenstände (tangible goods) beziehen kann.

In Frage kommt aber die Anerkennung einer eigentumsähnlichen Position an einem Immaterialgut. Juristen gehen allerdings überwiegend vom Bestehen eines numerus clausus der Immaterialgüter aus und erkennen nur die bereits gesetzlich geregelten Fälle (etwa:Werk/Urheberrecht; Erfindung/Patentrecht; Geheimnis/Know How-Schutz; Geschäftsgeheimnis) als proprietäre Rechte an. Eine eigentumsähnliches Recht an „Daten" wird in Deutschland deshalb bisher nicht anerkannt. Das sui generis – Recht an Datenbanken bezieht sich auf die Organisationsleistung, nicht auf die in der Datenbank gespeicherten Daten.

Deshalb wirdüberwiegend für „big data"- Sammlungen ein freier Zugang und eine freie Nutzung gefordert, also ökonomisch gesehen die Anerkennung der Daten als öffentliche Güter. Dadurch werden die Umstände der Entstehung und der Zuordnung von Informationen ausgeklammert. Es wird auf den faktischen Besitz abgestellt und das Nutzungsrecht an Informationen auf das kartellrechtliche

[54] Kerber, Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection, GRUR Int. 2016, 639 (https://papers.ssrn.com).

[55] Dorner, Big Data und "Dateneigentum". Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617; Kilian, Vom Recht auf eigene Daten, in: Frankfurter Allgemeine Zeitung vom 4.7.2014, S. 20; Strukturwandel der Privatheit, in: Garstka/Coy (Hrsg.), Steinmüller-Gedächtnisschrift, Berlin 2014, S. 195 (https://edoc.hu-berlin.de/handle/18452/18547).

Problem des Zugangs reduziert.[56]Die Gegenmeinung, die eigentumsähnliche Rechte anerkennenmöchte, beruft sich auf Funktionalitäten, Geschäftszwecke, Investitionen odereingesetzte technische Mittel, für die es aber außerhalb des numerus clausus der Immaterialgüterrechtebisher keinen Schutz gibt.Allerdingswäredie Schaffung eines neuen eigentumsähnlichen Rechts an marktfähigen Informationen denkbar, etwa in Anlehnung an das Urheberrecht oder an den Know How -Schutz, und zwar einschließlich dereninhärenten Schranken.

Vernachlässigt wirdbishersowohl von Ökonomen als auch Juristen die Tatsache, dass für die Teilmenge der personenbezogenen Daten (richtig eigentlich: „personenbezogene Informationen") bereits ein rechtliches Sonderregime in der Europäischen Union besteht, das zwingendes öffentliches Recht darstellt: Nach der Datenschutzgrundverordnung[57] hat der Betroffene ein Bündel von unabdingbaren Rechten gegen den Verantwortlichen für die Verarbeitung seiner personenbezogenen Daten. Dieses Bündel an Rechten (Einwilligung; Auskunft; Änderung; Anonymisierung; Pseudonymisierung; Löschung; Portabilität) erzeugt eine Rechtsstellung, die ein hohes Datenschutzniveau verwirklichen helfen soll, wie es Art. 7 und 8 der Charta der Grundrechte der Europäischen Union und Art. 8 EMRH garantieren.

Diese Rechtsstellung wirkt sich vor allemim Bereich der Wirtschaft aus, denn im öffentlichen Bereich haben die öffentlichen Interessen an Sicherheit und Ordnung Vorrang vor den Individualinteressen.Die öffentlichen Interessen sind in Deutschland umfassend gesetzlich geregelt.Das jüngste Beispiel ist das Videoüberwachungverbesserungsgesetz[58], wonach hinsichtlich öffentlich zugänglicher Plätze oder Fahrzeuge die Videoüberwachung Vorrang vor Individualinteressen genießt.

Trotz solcher gesetzlichen Regelungenwird in der Politik und in der juristischen Fachöffentlichkeit oftüber den Ausgleich staatlicher Interessen einerseits und individuellen Freiheiten andererseits lebhaft gestritten. Das zeigt sich etwa an dem Konflikt über die Zulässigkeit und die Grenzen der anlasslosen Vorratsdatenspeicherung.[59]Auch nachdem der Europäische Gerichtshof die Vorratsdatenspeicherungsrichtlinie 2006/24/EG[60] für ungültig erklärt hatte, wurde in Deutschland die anlasslose Vorratsdatenspeicherung beibehalten. Ein Gesetz zur Einführung einer Speicherfrist für Verkehrsdaten[61]verkürzt lediglich die

[56] Drexl, Neue Regeln für die Europäische Datenwirtschaft? NZKart 8/2017, 415.
[57] Verordnung (EU) 2016/679 vom 27.4.2016 ABl. L 119 vom 4.5.2016,S. 1.
[58] Videoüberwachungsverbesserungsgesetz vom 28.4.2017 BGBl. I S. 968.
[59] TK-Überwachungs- und Vorratsdatenspeicherunggesetz vom....
[60] EuGH vom 8.4.2014, C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger/Minister for Communications, ECLI:EU:C:2014:238.
[61] Vom 10.12.2015 BGBl. I S. 2218.

Speicherfristenfür Internet- und Telekommunikationsdaten auf zehn Wochen und für Mobilfunkdaten auf vier Wochen.

Die deutschen Telekommunikationsunternehmen haben seitdem 1. Juli 2017 die Pflicht, Verkehrsdaten zu speichern, ohne dass ein Verdacht auf schwere Straftaten zu Grunde liegen muss.Eilanträge vor dem Bundesverfassungsgerichtgegen den Beginn der Speicherungen wurden abgelehnt und einer Entscheidung im schwebenden Hauptverfahren vorbehalten.[62]Das OVG Nordrhein-Westfalen hält die Verpflichtung zur Speicherung nicht für europarechtskonform.[63] Daraufhin hat die Bundesnetzagentur bekannt gegeben, dass sie bis zur endgültigen Klärung der Rechtsfrage keine Zwangsmaßnahmen gegen TK-Unternehmen ergreifen wird, die eine Speicherung verweigern.[64]Die im Vorratsdatenspeicherungsgesetz eingeführte Überwachungsmöglichkeit hinsichtlich Personen, die einem Berufsgeheimnis unterliegen, wurde inzwischen durch § 29 Abs. 3 BDSG 2017 wieder rückgängig gemacht.

Die in der Praxis oft stattfindende Verknüpfung von personenbezogenen Daten mit anderen Daten („Industriedaten“) stellt kein triviales Problem dar. Deshalb wird in der Praxis das Datenschutzrecht oftnicht beachtet oder es wird rechtspolitisch gefordert[65], die dem Datenschutzrechtzu Grunde liegenden Prinzipien umzukehren:Jede Form der Datenverarbeitung solle erlaubt werden, wenn sie nicht im Einzelfall ausdrücklich verboten sei. Dies ist bei den Verhandlungen zum TiSA-Abkommen[66]unter anderem die Verhandlungsposition der U.S.A. und Australiens und war überraschender Weise auch die Position der deutschen Bundesregierung bei den Beratungenzur Datenschutzgrundverordnung, mit der sie aber nicht durchgedrungen ist.[67]Dass es grundsätzlich technisch möglich ist, personenbezogene Daten von anderen Daten zu trennen und jeweils unterschiedliche rechtliche Rahmenbedingungen dafür zu entwickeln, zeigt das Beispiel des europäischen Notrufs (E-call).[68]

[62] BVerfG vom 26.3.2017, 1 BvR 141/16

[63] Az. 13 B 238/17 vom 22.6.2017 (www.justiz.nrw.de), besucht am 30.8.2017.

[64] DuD 2017, 596.

[65] Härting/Schneider, Ein Alternativentwurf für eine Datenschutz-Grundverordnung (An Alternative Draft for a General Data Protection Regulation),
Computer Law Review International, January 2013, Supplement 1.

[66] Trade in Services Agreement, vgl. Kilian, International Trade Agreements and European Data Protection Law, CRi 2016, 51.

[67] Albrecht, Hände weg von unseren Daten, München 2014.

[68] Durchführungsverordnung (EU) 2017/78 vom 15.7.2016 ABl. L 12 vom 17.1.2017, S. 26; a.A: Drexl, Neue Regeln für die Europäische Datenwirtschaft? NZKart 8/2017, S. 415 (416).

Frage 4.1.

Die Datenschutzgrundverordnung[69] wurde durch ein Rahmengesetz, das Datenschutz- Anpassungs- und -Umsetzungsgesetz[70], legislativ in das deutsche System des Datenschutzrechts überführt. Das bisherige Bundesdatenschutzgesetz wurde neu gefasst. Zugleich setzte das Rahmengesetz die Strafverfolgungs-Datenschutzrichtlinie[71] in deutsches Recht um.

Bei der Umsetzung fiel auf, wie stark die Vorbehalte gegenüber den bewährten Prinzipien des Datenschutzes in der größten Regierungspartei CDU sind. Die Debatte im Deutschen Bundestag dauerte nur 40 Minuten. Während die Oppositionsparteien die europäischen Verschärfungen des Datenschutzrechtes einhellig begrüßten, ging die Regierungeher auf Distanz. Das zuständige Bundesinnenministerium hatte bereits bei den Beratungen im Rat der Europäischen Union auf eine Verwässerung des Datenschutzrechts gedrängt und lange Zeit die Beratungen zur Datenschutzgrundverordnung gebremst[72].

In der Bundestagsdebatte zum deutschen Anpassungsgesetz sagte Bundesinnenminister de Maizière: „'Das Verständnis eines Datenschutzes im Sinne möglichst großer Datensparsamkeit hat sich auch durch die technische Entwicklung überholt"[73]. Das widersprichtklar der Rechtslage, denn sowohl Art. 5(1)(c) DSGVO als auch der Europäische Gerichtshof in seinem Gutachten zum EU-Fluggastabkommen mit Kanada[74] bekräftigen die Datenminimierung als einen wichtigen Grundsatz des Datenschutzrechts. In dieserBundestagsdebatte sagte der Minister weiter: „Wenn nicht in Europa die Datenschätze gehoben, analysiert, zu wertvollen Informationen veredelt und klug genutzt werden, dann werden es andere tun. Die anderen werden es aber nicht auf dem Niveau der Europäischen Union machen".[75] Diese Feststellung erstaunt noch mehr, dennsieunterscheidet nicht zwischen personenbezogenen Daten und anderen Daten, erwähnt nicht das Marktortprinzip für die Anwendung des europäischen Datenschutzrechts, stelltimplizit das Zweckbindungsprinzip in Frage undmisst anscheinend dem neuen Sanktionensystem der Datenschutzgrundverordnung zur Beachtung des Datenschutzrechtsgeringe Bedeutung zu.

An mehreren Stellen schwächt das deutsche Anpassungs- und Umsetzungsgesetz Rechte des Betroffenen ab, was europarechtswidrig sein könnte: Während

[69] VO (EU) 2016/679 vom 27.4.2016 ABl. L 119 vom 4.5.2016, S. 1.

[70] DSAnpUG-EU vom 30.6.2017 BGBl. I S. 2097.

[71] Richtlinie (EU) 2016/680 vom 27.4.2016 ABl. L 119 vom 4.5.2016, S. 89.

[72] Albrecht, Hände weg von unseren Daten, München 2014 (Albrecht war Rapporteur des Europäischen Parlaments für Datenschutz).

[73] Plenarprotokoll 18/221, 221. Sitzung vom 9.3.2017, TOP 11 zu BT-Drs. 11401, S. 22177.

[74] Gutachten 1/15 vom 26.7.2017, Rdnr. 140.

[75] Tagesordnungspunkt 11 zu BT-Drs. 18/11401 vom 9.3.2017, S. 22177.

nach Art. 82 Abs. 1 DSGVO jeder Verantwortliche für materielle oder immaterielle Schäden, die von ihm verursacht worden sind, unabhängig vom Verschulden auf Schadenersatz haftet – es sei denn, er kann beweisen, dass er in keinerlei Hinsicht eine Schadensursache gesetzt hat (Art. 82 Abs. 3 DSGVO) – muss nach § 83 Abs. 4 BDSG 2017 ein Mitverschulden der betroffenen Person bei der Entstehung des Schadens berücksichtigt werden.Dadurch wird die modifizierte EU-Gefährdungshaftung für eine generell bestehende Risikolage einer Verschuldenshaftung angenähert. Ferner kann nach den neuen deutschen Regelungen bei der Weiterverwendung personenbezogener Daten die Informationspflicht entfallen (§§ 32, 33 BDSG 2017). Bei hohem technischen Aufwand und geringem Interesse der betroffenen Person fällt auch das Recht auf Löschung (§ 35 BDSG 2017) weg. Im Rahmen einer Leistungserbringung nach einem Versicherungsvertrag sind automatische Profilbildungen zulässig (§ 37 BDSG 2017).

Im Gesetzgebungsverfahren hat der Bundesrat (Länderkammer) einige Verbesserungen gegenüber dem ursprünglichen Regierungsentwurf durchgesetzt. So enthält das neugefasste Bundesdatenschutzgesetz erstmals Grundsatzregelungenfür Beschäftigte (§ 26 BDSG 2017).Bei der Umsetzung der Strafverfolgungsrichtliniewurde die ursprünglich vorgesehene Kontrollmöglichkeit von Berufsgeheimnisträgern durch öffentliche Stellenwieder zurückgenommen.

Frage 4.2.

Die deutschen Unternehmen passen bereits jetzt das interne Controlling an die Vorschriften der ab Mai 2018 geltenden Datenschutzgrundverordnung an. Das betrifft vor allem die Notwendigkeit der Einführung von Verfahren zur Datenschutz-Folgenabschätzung (§ 67 BDSG 2017), Dokumentationsverfahren über die Grundlagen, Zwecke, Empfänger personenbezogener Daten, die Verwendung von Profilen sowieder Einführung technischer und organisatorischerSchutzmaßnahmen.

Auf dem privaten Fortbildungsmarkt werden zahlreiche neue Ausbildungslehrgänge für Datenschutz- und IT-Recht angeboten. Sie tragen Bezeichnungen wie „operativer Datenschutz“, „IT-Compliance“, „Datenschutz-Governance“und richten sich an verantwortliche Mitarbeiter von Unternehmen. Veranstaltet werden solche Kurse von großen Verlagen, Rechtsanwaltskanzleien, berufsbezogenen Organisationen sowie kommerziellen Anbietern. Soweit Hochschullehrer beteiligt sind, werden manchmal Hochschulzertifikate verliehen. Sie liegen unterhalb der Schwelle akademischer Grade und schwanken in ihrerAussagekraft je nach Veranstalter und Qualität derAngebote.

Zuverlässiger einzuschätzen sind Fortbildungsnachweise, die nach § 15 der deutschen Fachanwaltsordnung (FAO) für die Berufsbezeichnung „Fachanwalt Informationstechnologierecht“ zu erbringen sind unddie von den Rechtsan-

waltskammern anerkannt werden müssen. Am 1.1.2017 gab es 556 Fachanwalte (-innen) für Informationstechnologierecht in Deutschland.[76]Alle größeren Anwaltskanzleien unterhalten inzwischen spezielle Gruppen für IT- und Datenschutzrecht und sehen darin einen wachsenden Geschäftsbereich, wie schon eine flüchtige Durchsicht der aktuellen Stellenangebote zeigt.

Die Tätigkeit von betrieblichen Datenschutzbeauftragten hat in Deutschland Tradition und trifft deshalb auf allgemeine Akzeptanz. Ein spezielles Qualifikationsprofil für die Datenschutzbeauftragten besteht bisher allerdings nicht. Die Aufgabe wird meist von Juristen, Informatikern oder leitenden Angestellten wahrgenommen.Diese sind überwiegend Mitglieder in großen privaten Fachorganisationen.[77]

Frage 4.3.

Die technische Möglichkeit, körperliche Dinge durch Zuordnung von Identifikationsnummern über ein eigenes „Internet der Dinge" zu verknüpfen, wird in Deutschland schon länger praktiziert. Seit mehreren Jahren kann man auf der weltgrößten Computermesse CEBIT in Hannover Anwendungsbeispiele sehen. Es geht hier um integrierte sensorenbasierte Produktionsverfahren, bei denen Messwerte bestimmte Reaktionen bei kommunizierenden Geräteteilen auslösen. Die steuernde Software beruht bei den einfacheren Systemen auf Konditionalprogrammen. Je mehr Variablen aber in die Algorithmen eingebaut werden, umso mehr Freiheitsgrade für potenzielle Reaktionen bestehen. Lernfähigen Algorithmen werden meist mit „Künstlicher Intelligenz" (artificial intelligence, AI) ausgestattet angesehen.

Dieses aus der Industrieperspektive „Industrie 4.0" bezeichnete Modell einer digitalisierten Produktion wächst mit dem künftigen Internet der Dinge (IoT) zusammen.[78]Beim Internet der Dinge geht es nicht nur um die industriegetriebene Produktion, sondern auch um Möglichkeiten der informationstechnischen Vernetzung von Instrumenten im privaten Bereich, wie etwa die WLAN-Verknüpfung technischer Geräte in einem Haus („smart home") oder die Messungen des Energieverbrauchs einzelner Haushaltsgeräte („smart metering"). Das Zusammenwachsen der digitalisierten Produktion mit der privaten Nutzung vernetzterGeräte lässt sich gut am Beispiel eines (semi-) autonomen Fahrzeugs studieren.

In politischer Hinsicht steht in Deutschland die Förderung von „Industrie 4.0" im Vordergrund. Ziel ist es, eine starke Individualisierung der Produkte

[76] Statistik der Bundesrechtsanwaltskammer (www.brak.de).

[77] Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)-https://www.gdd.de; Deutsche Gesellschaft für Recht und Informatik e.V (DGRI)- https://www.dgri.de; https://www.dgri.eu.

[78] https://www.bmft.de/de/zukunftsprojekt-industrie-4-0-848.html

unter den Bedingungen einer hoch flexibilisierten (Großserien-) Produktion zu ermöglichen. „Mit intelligenten Monitoring- und Entscheidungsprozessen sollen Unternehmen und ganze Wertschöpfungsnetzwerke in nahezu Echtzeit gesteuert und optimiert werden können".[79] Ein Förderetat des Bundesministeriums für Bildung in Höhe von 470 Mio. Euro steht bis Ende 2017 zur Verfügung. Eine zusätzliche Förderinitiative des Bundesministeriums für Wirtschaft und Energie unterstützt kleine und mittlere Unternehmen (KMU) dadurch, dass autorisierten Beratungsunternehmen, die den kleineren Unternehmen bei der digitalen Markterschließung helfen, einen Teil der Kosten erstattet werden.[80] Der Umsatz mit „Industrie 4.0" in Deutschland wird von 5,8 Mrd. Euro im Jahre 2017 auf 7,2 Mrd. Euro im Jahre 2018 steigen.[81]

Im Juni 2017 wurde zwischen Deutschland, Frankreich und Italien eine trilaterale Kooperation zur digitalen Produktion vereinbart, bei der es um die Standardisierung der Referenzarchitektur und Erfahrungsaustausch geht.[82]

In rechtlicher Hinsicht geht aufgrund empirischer Untersuchungen die Vermutung von Industrieunternehmen dahin, dass Datenschutz und Datensicherung die Hauptprobleme bei „Industrie 4.0" bilden.

Der Datenschutz war bisher – soweit ersichtlich – weder in den Bereichen „Industrie 4.0" noch bei „IoT" Gegenstand eines Rechtsstreits in Deutschland.

Die Datensicherung im Bereich „Industrie 4.0" liegt im Eigeninteresse der Unternehmen, um den Abfluss von Kow How und Geschäftsgeheimnissen zu verhindern. Der Grad an Datensicherung ist kostenabhängig und kann zwar beliebig gesteigert, das Risiko für Angriffe aber dennoch nicht völlig ausgeschlossen werden.Verbindliche Modelle für die Intensität der Datensicherung bestehen in Deutschland für den öffentlichen Bereich, verbindliche allgemeine (technisch noch nicht spezifizierte) Rechtsvorschriften für alle Bereiche, soweit es sich um personenbezogene Daten handelt(Art. 5(1)(f) DSGVO).Zusätzlich können versicherungsrechtliche Obliegenheitspflichten bestehen.

Vereinbarungentechnischer Standards für Produktionsverfahren fallen in der Regel unter die EU-Gruppenfreistellungsverordnung für Forschung und Entwicklung[83] und sind kartellrechtlich unbedenklich.

Frage 4.3.1.

Die meisten deutschen Haushalte verfügen über etliche elektronische Geräte (Smartphones; Computer; Smart TV; Spielkonsolen), die über WLAN verknüpft

[79] https://www.bmft.de/de/zukunftsprojekt-industrie-4-0-848.html
[80] www.bmwi-go-digital.de
[81] www.bitkom.org
[82] www.plattform-i40.de
[83] Verordnung (EU) Nr. 1217/2010 vom 14.12.2010 ABl. L 335 vom 18.12.2010, S. 36.

sind. Die Deutsche Telekom (wie auch sechs weitere EU-Staaten, nämlich: Niederlande; Griechenland; Kroatien; Österreich; Polen und Slowenien) führen dafür seit 2017 die Funktechnik „Narrow-IoT“ im 800 oder 900 Mhz-Band kommerziell ein. Das ist die Grundlage für die Erfassung, Visualisierung und Verwendung von Gerätedaten. Hierfür sind vor allem die datenschutz- und verbraucherrechtlichen Vorschriften zu beachten.

Frage 4.3.2.
Rechtliche Probleme werden in Deutschland im Bereich „IoT“ werden vor allem im Hinblick auf „smart metering“ diskutiert.

Mit dem Ausstieg aus der Atomenergie und der Hinwendung zu erneuerbaren Energien steigt der Bedarf an Kontrollsystemen zur Steuerung einer zuverlässigen Energieversorgung. Stattet man Verbrauchsgeräte (etwa Kühlschränke; Waschmaschinen, Fernsehgeräte, Computer) mit einem Chip aus, der das Gerät kennzeichnet, den Verbrauch misst und die Messdaten weitermeldet, ist es möglich, den Stromverbrauch pro Person, Gerät, Zeitintervallund Wohneinheit zu ermitteln. Das kann für den Verbraucher den Anreiz bieten, stromsparendere Geräte einzusetzen. Wenn dieEnergieversorgungsunternehmen für die Abrechnung des Stromverbrauchs die Angaben des Verbrauchs der einzelnen Geräte erhalten, können sie durch Sekundärauswertungen Werbung betreiben oder Dienstleistungen anbieten, da die Daten personenbeziehbar sind. Die Daten über die Dauer und Einschaltzeit eines „Smart TV“-Gerätes lässt beispielsweise intensive Rückschlüsse über die Fernsehpräferenzen und das Konsumverhalten des Kunden zu.

Deshalb werden in Deutschland „smart metering – Verfahren intensiv unter Datenschutzaspekten diskutiert. Da pseudonyme oder anonyme Verbrauchsabrechnungen nicht möglich sind, sollten Regelungen de lege ferendasicherstellen, dassnur der Gesamtstromverbrauch an das Energieversorgungsunternehmen weitergemeldet werdendarf, es sei denn, der Verbraucher willigt in die Weitergabe der Verbrauchsdaten seiner Einzelgeräte ein („Optin“-Verfahren).

Frage 4.3.3.
Ein weiterer Bereich in der juristischen Diskussion in Deutschland bieten die (semi-) autonomen Fahrzeuge, wie sie bei allen deutschen Autoproduzenten in der Planung sind[84]. Nach der Tötung von drei Personen durch ein mit Assistenzsystemen ausgestattetes Fahrzeug in Süddeutschland im Jahre 2015, dessen Fahrer einen Herzinfarkt erlitten hatte, wurde die Diskussion in alle Richtun-

[84] Oppermann/Stender-Vorwachs (Hrsg.), Autonomes Fahren. Rechtsfolgen, Rechtsprobleme, technische Grundlagen, München 2017.

gen vertieft.[85] Im Vordergrund stand bisher die Spezifizierung der Produkt- und Produzentenhaftung auf der Grundlage der Programmierung der Fahrzeuge.[86]

Aus technischer Sicht ist eine autonome Überwachung der Fahrzeugfunktionen durch Sensoren im Fahrzeug geplant, was die Erhebung und Auswertung vieler Daten erforderlich macht. Die Hersteller sollen gewährleisten, dass die Programme aufgrund der Protokolldaten selbst einen sicheren Zustand wieder herbeiführen oder dem Fahrer genügend Zeit für ein Eingreifen lassen. Bei selbstlernender Software sollendeshalb hohe Qualitätsanforderungen an die Programmierung gestellt werden. Gefordert wird auch, einen „Crash-Optimierungs-Algorithmus" für Dilemma-Situationen vorzusehen, was ethische Probleme aufwirft, wenn etwa zwischen der Tötung von einer Person auf der einen oder zwei Personen auf der anderen Straßenseite zu entscheiden ist. Die Möglichkeit einer Risiko-Nutzen- Abwägung ist zweifelhaft.

Stets wird ein GPS-System für die Lokalisierung eines (semi-) autonomen Fahrzeugs eingesetzt, was regelmäßig dazu führt, dass die anfallenden Daten einen Personenbezug aufweisen. Wie die EU-Durchführungsverordnung 2017 zum E-Call System[87] zeigt, ist es dennoch grundsätzlich möglich, die Fahrzeugdaten vom Personenbezug zu entkoppeln und dem Fahrzeugführer alternative Handlungsmöglichkeiten zu belassen.

Eine vom Bundesminister für Verkehr und digitale Infrastruktur eingesetzte interdisziplinäre Ethikkommission zum automatisierten Fahren hat im Juni 2017 ihren Bericht in 20 Thesen zusammengefasst. Die fünf Kernpunkte lauten wörtlich:

- Das automatisierte und vernetzte Fahren ist ethisch geboten, wenn die Systeme weniger Unfälle verursachen als menschliche Fahrer (positive Risikobilanz).
- Sachschaden geht vor Personenschaden: In Gefahrensituationen hat der Schutz menschlichen Lebens immer höchste Priorität.
- Bei unausweichlichen Unfallsituationen ist jede Qualifizierung von Menschen nach persönlichen Merkmalen (Alter, Geschlecht, körperliche oder geistige Konstitution) unzulässig.
- In jeder Fahrsituation muss klar geregelt und erkennbar sein, wer für die Fahraufgabe zuständig ist: Der Mensch oder der Computer. Wer fährt, muss dokumentiert und gespeichert werden (u.a. zur Klärung möglicher Haftungsfragen).

[85] Hilgendorf, Forschung und Lehre, 6/16, S. 480.

[86] Ebers, Autonomes Fahren. Produkt- und Produzentenhaftung, in: Oppermann/Stender-Vorwachs (Hrsg.), München 2017, S. 93.

[87] Delegierte Verordnung (EU) 2017/79 vom 12.9.2016 ABlEU L 12 vom 17.1.2017, S. 44.

- Der Fahrer muss grundsätzlich selbst über Weitergabe und Verwendung seiner Fahrzeugdaten entscheiden können (Datensouveranität).[88]

Der deutsche Gesetzgeber hat im Juni 2017 einige Problempunkte durch Änderungen des Straßenverkehrsgesetzesgeregelt.[89]Kraftfahrzeuge mit hoch- und vollautomatischen Fahrfunktionen sind zulässig, wenn sie den Verkehrsvorschriften entsprechen und wenn sie jederzeit durch den Fahrzeugführer manuell übersteuerbar oder deaktivierbar sind (§ 1a Abs. 3 STVG). Ein Fahrzeugführer darf sich abwenden, wenn das Fahrzeug automatisch fährt. Er muss aber die Steuerung übernehmen, wenn das System ihm das optisch, akustisch oder sonst wahrnehmbar anzeigt (§ 1b StVG).

Bei einem Wechsel der Fahrzeugsteuerung zwischen dem hoch- oder vollautomatisierten System und dem Fahrzeugführer oder wenn eine technische Störung eintritt speichert das Satellitennavigationssystem die ermittelten Positions- und Zeitangaben (§ 63a Abs. 1 STVG). Die gespeicherten Daten dürfen zur Ahndung von Verkehrsverstößen den zuständigen Behörden (§ 63a Abs. 2 STVG) und in anonymisierter Form auch zum Zwecke der Unfallforschung (§ 63a Abs. 5 STVG)übermittelt werden. Die GPS-Daten dürfen durch den Fahrzeughalter an Dritte zur Geltendmachung, Befriedigung oder Abwehr von Rechtsansprüchen weitergegeben werden. Bemerkenswert ist, dass im Gesetz keine Weitergabe der Daten an den Fahrzeughersteller vorsieht.

Frage 4.4.

Das Ergebnis des Urteils des Europäischen Gerichtshofs im Fall Google/Spanien[90] ist in Art. 17 (2) der EU-Datenschutzgrundverordnung (DSGVO) verankert und somit ab 25.Mai 2018 einheitlich geltendes Unionsrecht. Das Bundesdatenschutzgesetz 2017 (BDSG 2017) hat in § 35 ergänzende Klarstellungen vorgenommen. So entfällt eine Löschung, wenn satzungsgemäße oder gesetzliche Aufbewahrungsvorschriften bestehen (§ 35 Abs. 3 BDSG 2017). An Stelle einer Löschung tritt eine eingeschränkte Verarbeitung nach Art. 18 DSGVO, wenn der Verantwortliche Grund zur Annahme hat, dass schutzwürdige Interessen der betroffenen Person verletzt würden(§ 35 Abs. 2 BDSG 2017).

Das nach Art. 6 und 12 (b) der Richtlinie 95/46/EG und das nach § 35 des bisherigen BDSG geltende Recht auf Löschungwird in Deutschland sehr stark genutzt. Nach dem jüngsten Transparenzbericht von Google wurden bisher weltweit 588 769 Ersuchen auf Entfernung von URLs (hauptsächlich von Facebook

[88] www.bmvi.de/bericht-ethikkommission; https://www.bmvi.de/SharedDocs/DE/Anlage/Presse/084-dobrindt-bericht-der-ethik-kommission.html?nn=12830 (aufgesucht am 30.8.2017).

[89] 8. Gesetz zur Änderung des Straßenverkehrsgesetzes (8. StVGÄndG) vom 16.6.2017 BGBl. I S. 1648.

[90] EuGH, 13.5.2014, C-131/12, ECLI:EU:C:2014:317.

und Youtube) gestellt, davon kamen 66 198 aus Deutschland. Von den deutschen Ersuchen wurden 48,2% stattgegeben.[91]

Über anhängige oder entschiedene Klagen vor deutschen Gerichten gibt es noch keine Statistik. Jedoch sind mehrere Klagen vor Landgerichten sowie eine vor einem Oberlandesgericht bekannt geworden.[92]Das LG Hamburg hat ein Löschungsbegehren gegen die Google Deutschland GmbH abgelehnt, weil diese Gesellschaft nicht selbst speichere. Es wurde keine datenschutzrechtliche Prüfung, sondern eine zivilrechtliche Interessenabwägung nach Deliktsrecht durchgeführt.[93]Das LG Frankfurt hat im Jahre 2016 eine Klage auf Löschung von sieben URLs aus der Google-Trefferliste an die Google Inc. in den U.S.A. zugestellt, und zwar ohne eine vorhergehende englische Übersetzung der Klageschrift zu fordern.[94]Ebenso hat das LG Frankfurt im Jahre 2017 die Google Germany GmbH als Störerin zur Unterlassung der angegriffenen Verlinkungen verpflichtet.[95]

Der Hamburgische Datenschutzbeauftragte hat 2017 durchgesetzt, dass Google Inc. personenbezogene Daten aus Verbraucher-Insolvenzverfahren grundsätzlich nicht mehr verlinkt.Solche Informationen sind zwar auf dem Behordenportal elektronisch öffentlich zugänglich, werden aber durch robots.txt-Dateien vor dem systematischen Zugriff durch Suchmaschinen geschützt.[96]Damit soll erreicht werden, dass privatinsolvente Personen nicht dauerhaft Schaden erleiden oder gezielt Marketingmaßnahmen ausgesetzt werden.

Der deutsche Dachverband für Verbraucherinteressen (Verbraucherzentrale) regt Internetnutzer dazu an, sich auf „die Suche nach sich selbst“ zu begeben („Egosurfing“; „Self-Googeling“) und bei veralteten Informationen bei Suchmaschinenanbietern die Löschung zu verlangen. Es wird ein Musterbrief für den Löschungsantrag in Suchmaschinen angeboten.[97]

Datenschutz und Verbraucherschutz sind damit in Deutschlandeng verzahnt, was wegen der Marktfähigkeit vieler personenbezogener Daten schon länger zu erwarten war.[98]Das hohe europäische Schutzniveau in beiden Bereichen und die

[91] www.google.com/transparencyreport/removals/europeprivacy (besucht am 4.9.2017).

[92] LG Wiesbaden, 10.3.2015, 4 O 7/15 (Berufung ist beim OLG Frankfurt anhängig); LG Hamburg, 11.2.2017 www.rechtsprechung-hamburg.de (mit einem Streitwert von 15 000 Euro).

[93] LG Hamburg, 28.8.2015

[94] https://ggr-law.com (besucht am 5.9.2017).

[95] LG Frankfurt ZD 2017, 391.

[96] https://www.datenschutz-hamburg.de (aufgesucht am 6.9.2017)

[97] https://www.verbraucherzentrale.de/recht-auf-vergessen (besucht am 5.9.2017).

[98] Kilian, Consumer Protection in the information and telecommunications sector. Current state and potential developments, in: Wydanictwo Uniwersitetu Wroclawskiego, Wroclaw 2011, 9-31 (spanische Übersetzung in: Revista de la Facultad de Derecho, Universidad de la Républica, No. 32, pp. 205-223, Montevideo 2012.

Einführung des Marktortprinzips durch Art. 3 DSGVOerzwingt inzwischen Anpassungsprozesse bei den global marktbeherrschenden US-Internet-Dienstleistungsunternehmen.[99]

[99] „Recent legal developments in Europe…resulted in some uncertainty, and compliance obligations could cause us to incur costs or require us to change our business practices in a manner adverse to our business" (https://abc.xyz/investor/pdf/2016_google_annual_report.pdf, p.8), besucht am 30.8.2017.

GREECE

Despina Anagnostopoulou*
Sylvia Stavridou**

1. Internal Market and electronic commerce: Internet and e-commerce
1.1. Electronic Commerce, liability of Internet intermediaries

Question 1.1.1.

Greece like most Member States has transposed literally the definitions of the E-Commerce Directive (ECD) as well as the activities and exemptions set in Articles 12 to 14. Therefore no specific liability exemptions have been adopted (e.g. for search engines, hyper-linking, blogs and social networks). This may lead to a regulatory uncertainty, taken into account other legal texts referring to ISS providers[1]. Apart from that there is no further clarification on the definition and

* Associate Professor, University of Macedonia. Responsible for answering questions 1.2.1.-1.2.7. on Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights, consumer protection and dispute resolution, 1.3.1. on geo-blocking, 1.4.1.-1.4.6. on Collaborative Economy and 4.1., 4.2. and 4.4. on Data in the Digital Economy.
** Assistant Professor, Democritus University of Thrace. Responsible for answering questions on 1.1.-1.4. on Electronic Commerce, liability of internet intermediaries, 2.1.-2.8. on Digital Media, 3.1.-3.4. on Digital Infrastructures and 4.3. on Internet of Things.

[1] Copyright Law No. 2121/1993 (Article 64A) provides for injunctions against "intermediaries" whose services are used by a third party to infringe a copyright or related right. Article 64A is transposing Article 11 of Directive 2004/48 (Enforcement Directive) and Article 8 (3) of Directive 2001/29 (Infosoc Directive) to Greek Law. Trade Mark Law No. 4072/2012 (Article 150 sec. 4) and Patent Law No. 1733/1987 (Article 17 sec. 1) provide for injunction against "intermediaries", transposing Article 11 of Directive 2004/48 (Enforcement Directive) to Greek Law. For telecommunication Law No. 3431/2006 (Article 2 sec. λα) (implementing Article 2 (m) of 2002/21/EC – Framework Directive) a provider of an electronic communication network is the entity establishing, operation, controlling or making available of an electronic communication network, or simply providing electronic communication services. According to Gambling Law No. 4002/2011 (Article 51 sec. 5) ISS providers shall deny access to on line gambling providers not subject to a priori permission through the competent National Regulatory Authority (Hellenic Gaming Commission).

the content of activities understood as intermediary services and those covered by the E-Commerce Directive exemptions[2].

Up to date Greek Courts dealt with ISS providers in few cases, mostly referring to copyright and personality rights infringements. In these cases the Courts considered the companies involved to be ISS providers and Articles 12, 14 ECD generally applied without proceeding to any further specification or delimitation of their activities (mere conduit, caching or hosting) and liability.

Internet access provider (telecommunication service provider): The Civil Court of Athens (First Instance, Cases 1639/2001, 2110/2002) considered the companies involved to be ISS providers without any further specification or delimitation of their activities (mere conduit, caching or hosting) and liability. In case 4658/2012 the Civil Court of Athens (First Instance), following the reasoning of CJEU in case C-557/07[3], considered that a mere internet access provider should be regarded as "intermediary" within the meaning of Article 8 (3) of Directive 2001/29 (Infosoc Directive).

Hosting: The Civil Court of Athens (First Instance, Case 457/2016) in a case concerning personality right infringement through offensive comments in blogs considered the company hosting such blogs (Google) as an ISS provider, supplying its clients with service of creating and managing blogs. In this case *the ISS provider was considered liable, although having already taken-down upon notice the illegal content, because it did not remove from the net all files stored containing the infringing text*. This additional measure[4], ordered by the Court ruling injunctions, is to ensure that the offensive text will not be reposted, *but results in disproportionate demands on intermediaries. This means that monitoring systems should have been implemented by the ISS provider searching all user – submitted information, which leads to the filtering of the whole content transmitted* (general filtering forbidden by Article 15 ECD).

File sharing services: The Penal Court of Athens (Court of Appeal, Case 6613/2016) initially considered a peer to peer file sharing service as a hosting service provider. Finally it did not apply the liability exemption considering that the owners and administrators of the file sharing service were fully aware that the files shared had been infringing others' copyright.

Search engines: The Civil Court of Athens (First Instance, Case 11339/2012) on a case dealing with personality infringement considered Google (providing search engine services) to be an ISS provider and ordered it to take adequate technical measures in order to disconnect defamation keywords from the name of the applicant.

[2] See also 3.4.2.1. Working Paper Commission, 2012.

[3] LSG v. Tele2, Case C-557/07, para. 46.

[4] Notice – and – stay down procedure, see Angelopoulos, https://www.ivir.nl/publicaties/download/Notice_and_Fair_Balance.pdf, page 17.

Blogs and social networks: The Court of Thrace (Court of Appeal, Case 91/2012) did not consider the blog owner – administrator falling under the liability exemptions of Articles 12-14 ECD. In this case the real identity of the blog owner – administrator could not be proven since its disclosure should conflict with privacy rules.

Question 1.1.2.

In case c-324/09 (L'Oreal) the Court specified further some conditions under which an ISP must be considered not to have played a "neutral role"[5] (by providing a merely technical and automatic processing of data), and therefore not to be subject to the general exemption of article 14 of e-commerce directive. The ISP plays an "active role" and therefore is deprived of the exemptions from liability provided for in Directive 2000/31, when it provides assistance which entails, in particular, optimizing the presentation of the offers for sale in question or promoting those offers (L'Oreal para 116, 123).

Even when having an operator who has not played an active role[6], it would not be exempt from liability, if it was aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality, and in the event of being so aware, failed to act expeditiously in accordance to Article 14(1)(b) of Directive 2000/31 (C- 324/09 L'Oreal v. eBay, para. 120, 122, 124).

As to the notice required for the awareness of an illegal activity or information the question remains on when a ISS provider is on notice of the illegal activity or information. The E-Commerce Directive requires no particular formalities leaving it to Member States and parties concerned on the basis of voluntary agreements (Recital 40 of Directive 2000/31/EC). In L'Oreal v. eBay the Court broadens the definition of awareness required by the ISS provider, as covering every situation in which the provider concerned becomes aware, in one way or another, of such facts or circumstances. In this perspective even a notification insufficiently precise or inadequately substantiated[7] may represent a factor taken into account to determine that the operator was actually aware of facts and circumstances (through the information transmitted to it) so to react as a "diligent economic operator" and identify the illegality (para. 122). The awareness required as a result of an investigation undertaken on its own initiative (para.

[5] "It is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores..." (Case C-236/08, Google Adwords, para. 114. "... That is not the case (neutral) where the service provider ... plays an active role of such a kind as to give it knowledge of, or control over, those data ..." (Case C-324/09, L'Oreal v. eBay, para. 113).

[6] According the criterion set by CJEU in Cases C-236/08 Google Adwords, para.114, C-324/09 L'Oreal v. eBay, para. 113, 123.

[7] The need to provide specific URL's makes it difficult for claimants, especially those who seek orders for infringing content to be taken down.

122) as well as a result of the identification of the illegality undertaken by the operator himself, based on simple information transmitted to him, imply a monitoring obligation for ISS providers.

It is also expected by the Commission that ISS providers hosting content should be in the future more preventive. This narrowing of immunity for service providers is also set out in Digital Single Market Strategy 2015 (par. 3.3.2.): "... the Commission will analyze the need ... whether to require intermediaries to exercise greater responsibility and due diligence in the way they manage their networks and systems ... a duty of care".

Furthermore a "diligent economic operator" may not just rely on the content of the notification received (which may be insufficient or inadequate) but furthermore should proceed to make an assessment about the legitimacy of the notice. Whether the activity or information concerned is indeed illegal or not, is not always so obvious and should be first answered by the national Courts.

The way the CJEU approaches the question of awareness of ISS providers being that of a "diligent economic operator" implies a general monitoring obligation and therefore requires a further clarification. To our opinion CJEU should nevertheless insist on the position taken in previous case (C-70/10 Sabam v. Scarlet) that filtering of all content constitutes general monitoring, and clarify that any investigation or identification undertaken by a ISS provider should be reduced to a particular content.

The precise factors and circumstances that will guide eventual liability for on line operators have been left to the national courts to determine. This may lead to different interpretation and implementation of this responsibility test, which put in to danger the legal uniformity required for the development of single digital market.

Question 1.1.3.

In addition to a notification and take-down procedure, action against repeat infringements as well as preventive measures are required[8]. As the information society expands and new forms of digital economy and activities appear, it has been shown that notice and take-down measures (Article14 ECD) may not be used uniformly but require diversification. In case of protection of minors (e.g. child pornography) inspection and automatic take-down by a ISS provider as well as additional measures to avoid any future distribution may be taken[9]. Apart from a general monitoring in the area of protection of minors (child pornography), as

[8] See Commission Staff Working Document, On line services including e-commerce, in the single market, 11/1/2012, SEC(2011), 1641 final. The commission will adopt a horizontal initiative on notice and action procedures.

[9] See also e.g. AVMSD Amendment Proposal, Article 28A sec. 2, below under Q.2.2.

to the measures undertaken the fair balance of rights in conflict should applied. In cases of severe harm or repeated harm a possible solution (oriented to the end user) could be the banning of the infringer from the intermediary's service.

In case of measures taken by the ISS provider without a prior judicial assessment on the illegality of a content or an activity, these measures should be more moderated[10], not so definitive and easy to recall in case that the assessment on illegality made by the ISS provider itself proves to be wrong[11]. Furthermore, since a previous judicial order is often time-consuming, a viable solution may be the setting of a competent Control Body (Committee for the notification of online copyright infringements[12]) as the one implemented by the Greek Copyright Law Amendment (Article 52 of Law No 4481/2017, which was transposed into the Greek Copyright Act (Law No 2121/1993) as Article 66E)[13]. Still the possibility to initiate judicial proceedings against the end – user may not be realistic since an injunctive order against the intermediary to disclose the end-user's identity should clash with data protection and (telecommunication) privacy issues.

In cases of hate speech the regime of notice-and-take down has already been adopted by the Commission and four major IT companies in a form of Code of Conduct and has been proven to be quite efficient[14].

Question 1.1.4.

In a copyright infringement case initially the court has pointed out (e.g. Court of Athens – First Instance – Case 4658/2012) that the application of Article 12 sec. 3 ECD (relevant Article 12 sec. 3 Presidential Decree No. 131/2003), does not conflict with Article 15 ECD (no general obligation to monitor) in case of injunctions ordered by national authorities or courts to ISS providers to terminate a particular and dully specified infringement. In contrary the notion of "prevention" is not clarified as to its content and extent. According to the above

[10] See also Proposal for a Directive on Copyright in the Digital Single Market (COM 2016, 593), Article 13 sec. 1 ("appropriate and proportionate").

[11] E.g. copyright or personality rights infringements, where the assessment on the illegality of a content or an action is more complicated for an ISS provider.

[12] Three –member Committee consisting of the chairman of the board of the Hellenic Copyright Organization, a representative of the Hellenic Telecommunications and Post Commission and a representative of the Hellenic Data Protection Authority.

[13] Although the time length of the proceeding set in Article 66E of Greek Copyright Law risks making the procedure uneffective.

[14] European Commission – Press Release (Brussels, 1 June 2017), Countering online hate speech – Commission initiative with social media platforms and civil society shows progress, available at http://europa.eu/rapid/press-release_IP-17-1471_en.htm. See also European Commission, 'Code of Conduct on Countering Illegal Hate Speech Online', available at http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf

Court decision the notion of prevention leads to the application of technological measures "filtering" the information transmitted in order to detect and prevent infringements. The Court follows the Recital 47 of ECD: monitoring obligations are accepted only in a specific case. Therefore deterioration or total block of access to peer to peer services in general may not be accepted since they may involve not only infringements but lawful uses as well. In this first case involving ISS providers the court held that the block of access to a particular and dully specified content (e.g. a specific site) is to be considered lawful (Court of Athens – First Instance – Case 4658/2012).

Apart from that as to the ordering of injunctions procedure, the request for a "take down" procedure has lead to controversial decisions. The most recent tendency is that courts deny a "take down" procedure[15]. Blocking in whole the access to specific sites where also legal content may be distributed is not compatible to the principle of proportionality[16] and clashes with the freedom of information, the freedom to conduct a business and the right to participate in information society. Any technical measure applied to protect a right should result from an ad hoc fair balance and it should take into account Article 1 of Directive 2002/21/EC (Framework Directive), as amended by Article 1 of Directive 2009/140/EC and (transposed in Telecommunication Law No. 4070/2013 Article 3 sec. 2 subsec. ζ')[17].

1.2. Consumer protection in relation to the Internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.

The Greek Law 3043/2002[18] has transposed almost all provisions of Directive 1999/44/EC (hereafter referred as CSD-Consumer Sales Directive) of minimum harmonization, in the old Civil Code of Greece (hereafter CC), by amending articles 534-537 CC, 540-561 CC and 332 and 334 CC. The Greek Law *did not differentiate between any types of contracts* since the legislator did not want to create any confusion or market fragmentation[19]. Only the provisions on commercial guarantees were separated and transposed with art. 5 par. 3-5 of the Consumer Protection Law 2251/2994.[20]

[15] Civil Court of Athens, First Instance, Cases No 13478/2014, 10452/2015.

[16] In Case No 13478/2014 the Civil Court of Athens (First Instance) following CJEU in case C-557/07 (LSG v. Tele2) points out that a consistent interpretation of relevant directives (2000/31, 2001/29, 2002/58 and 2004/48) must not conflict with fundamental rights and general principles of Community Law, such as the principle of proportionality.

[17] For the scope of net neutrality and the nature of the measures taken, see below under Q.3.1.

[18] Published in Official Journal (FEK) A' nº 192 dated 21 August 2002 p. 3745.

[19] See Preamble of the Law, A.I.3.

[20] Published in Official Journal (FEK) A' nº 191 dated 16 November 1994.

Two Greek provisions were found not to be in conformity with the Consumer Sales Directive (CSD) and were abolished in 2010: a) the *exclusion of the liability of the seller* in case the buyer received the product without reservation in knowledge of non-conformity (art. 545 CC) and b) the *exclusion of the buyer's rights if the seller* had set a reasonable period for the buyer to ask for replacement or for the rescission of the contract and the buyer had missed the deadline (art. 546 par. 2-3 CC).[21]

When Greek courts examine disputes on remedies, they confront the following problems:

A.The concepts of material defect and promised quality which are equivalent to non-conformity: According to art. 534 CC "the seller has the obligation to deliver the product with the qualities agreed without any material defects". According to art. 535 CC "the seller does not comply with the above oligation if the product delivered to the buyer is not in conformity with the product and in particular" presents the four problems (criteria of non-conformity) mentioned in the Directive 1999/44/EC (art. 3). Thus the Greek courts continue to have to define the concepts of material defect and lack of promised quality "at the time of passing of risk to the buyer" (art. 535 CC) without using the non-conformity criteria of the Directive[22], since the abovementioned concepts are considered to be synonym with non conformity[23]. There is no need to prove the fault of the seller (objective liability) according to art. 537 CC.

Material defect is "any imperfection on the composition or the position of the product that deprives or diminishes its value or usefulness in a substantial degree"[24] (art. 534 CC). In order to determine that there is a material defect, the court has to take into account the common understanding in the particular trade and not the subjective opinion of the buyer, except if the parties have already defined themselves the concept of material defect in their contract[25].

The *agreed quality* (or promised quality) refers to a certain physical attribute or advantage of a product and any relationship that, by its nature and duration, will positively affect its value or usefulness in accordance with the contract and the objective perception of transactions. The concept of "agreed quality" is based

[21] In 2010, the Law 3043/2002 was amended by article 16 of Act 3853/2010 under the title "the correct transposition of Directive 1999/44/EC".

[22] See judgment 2256/2015 One Member Court of Appeal of Thessaloniki.

[23] Christianopoulou, op.cit., p. 86.

[24] See Judgments of the Supreme Court no 29/1990 (Plenary Session), 1544/2008, 2216/2014, 1596/2014 and 267/2015. See also Judgment of the Court of Appeals of Athens 6910/2007, published at Elliniki Dikaiosyni, tome 49, p. 618.

[25] Judgments of the Court of Appeals of Thessaloniki 1710/2003, published in Armenopoulos 2004, p. 1665, and no 1085/1995, Armenopoulos 1995 p. 760.

on the explicit or implicit agreement between the parties[26] that the buyer gives particular importance to certain and specific technical properties or qualifications of the object of the contract and the seller guarantees their existence and is liable for their eventual lack.[27]

B. The free choice of the buyer on remedies: Art. 540 of the Greek Civil Code on "Buyer's rights" describes the rights among which the buyer can freely choose against the seller. In contrast to all other member states, three states (Greece, Portugal and Slovenia) have opted not to follow the "Hierarchy of Remedies" model, which consists of two stages: At the first stage, the buyer asks the seller to correct or replace, and if this is not possible, then he/she proceeds to the second stage to ask for price reduction or rescission of the contract (art. 3 of the Directive). Art. 540 CC provides that if the seller is liable for a defect or lack of an agreed quality, the buyer has the right, according to his/her free choice[28] to request from the seller any remedy provided by CSD 1999/44/EC (art. 3 par. 3-6): to repair or replace the product with another one except if such action is impossible or demands disproportional expenses by the seller; *or* to reduce the price; *or* to proceed to the rescission of the contract, if there is a *major* material defect or *any* lack of agreed quality[29]. This is called a selective accumulation of claims (eklektiki syrroi)[30]. The Supreme Court of Greece recognizes that the national provision is more favourable to the buyer than the CSD[31] and that the buyer has a free choice to exercise any of the above rights, even in case that the seller asks him to pay the price and the buyer *objects* by invoking price reduction.[32]

Under the prevailing opinion and the case law of the courts, the buyer had the right to choose only once which remedy to exercise and such declaration was considered "irrevocable" except if the repaired product was still not in conformity and the buyer proceeded to rescission of the contract[33]. The irrevocable character of the buyer's declaration was based on the general provision of art. 306 CC applied on accumulation of claims stating that the choice of the creditor can be made only once. In 2016 however, the Supreme Court invoked the provisions of the Directive 1999/44/EC in order to rule that the buyer's declaration is

[26] Judgments of the Supreme Court of Greece no 267/2015, 1381/2013, 575/2013, and 654/2012.
[27] Judgments of the Supreme Court of Athens 267/2015, 1381/2013, 575/2013, 654/2012.
[28] Judgment of the Court of Appeals of Thessaloniki, 2256/2015.
[29] The buyer may proceed to the rescission of the contract in case of lack of promised quality without having to prove that this lack was substantial. See P. Kornilakis, Concise Special Contract Law, 2nd Edition, Thessaloniki 2013, Sakkoulas publishers, p. 109.
[30] P. Kornilakis, op.cit., p. 117.
[31] Judgment of the Supreme Court 1636/2014.
[32] Judgment of the Supreme Court 596/2015.
[33] Judgment of the Supreme Court 243/2009 and One Member Court of Ioannina, 69/2011.

revocable[34]. The Supreme Court ruled that in case "the first request of the buyer is the replacement of the defective product, his/her choice, *as interpreted under the light of the Directive*, is not "irrevocable" and does not eliminate without any consideration his/her right to request price reduction or the rescission of the contract, in case that the seller refuses or does not proceed to the replacement in reasonable time".[35]

C. Review of the Greek courts of the right to rescission and its abusive exercise: The buyer's choice of rescission of the contract may be reviewed by the courts either by art. 542 CC or by art. 281 CC: a) Art. 542 CC limits the right of the consumer to proceed to rescission: Even though the buyer has exercised the right to have the contract rescinded, the court has the power to order only a price reduction the replacement of the product instead of contract rescission if it considers that the circumstances [of the specific case] *do not justify the rescission*". Circumstances that are taken into account by the court's own motion are the size and the importance of the defect or the lack of promised quality, the possibility of reselling the product and the disproportion between the benefit of the buyer to the loss of the seller.[36] This provision reflects the principle of good faith and honesty that must prevail in transactions.[37]

b) The Greek courts have the authority to refuse rescission of the contract in case that the buyer abuses this right in violation of *bona mores* and good faith according to art. 281 CC.[38] For the purposes of that general provision for any civil right, the long period of inactivity of the buyer, even if he has given the seller the impression that he will not exercise his right, does not render abusive his subsequent exercise unless it is accompanied by special circumstances that justify the sacrifice of the buyer's claim in order to avoid burdensome consequences for the seller according to good faith and bonas mores[39].

D. Review of the Greek courts of the right to replacement and its abusive exercise: There is a solid case law approved by the Greek Supreme Court that article 542 CC can be used by analogy in case that the buyer asks the replacement of the product, since the replacement of the contract resembles the rescission of the contract. Thus the Courts may order reduction of the price instead of replacement.[40]

[34] Judgment of the Supreme Court 1636/2014. See also art. 3 par. 5 of the Directive 1999/44/EC.

[35] The Supreme Court based its argument also on art. 541 CC providing thta in case the buyer discovers *another defect,* the buyer is entitled to exercise *ab novo* one of the rights of art. 540 CC. See also Judgment of the Supreme Court 575/2013.

[36] P. Kornilakis, op.cit., p. 142.

[37] Judgment of One Member Tribunal of Thessaloniki no 2722/2014.

[38] Art. 281 CC provides that the exercise of a right is prohibited if it manifestly exceeds the limits imposed by good faith or the bonas mores or the social or economic purpose of the right.

[39] Judgments of the Supreme Court of Greece 8/2001 (Plenary session), and 1799/2006.

[40] Judgment of the Supreme Court of Greece 996/2015. See also Judgment of One Member Tribunal of Thessaloniki no 2722/2014.

E. The right to price reduction: There is a consolidated case law that the buyer must prove: a) the existence of the contract of sale, b) the existence of the material defect or lack of agreed quality, c) the liability of the seller, irrespective of the seller's fault, for the defect existing when the risk passes to the buyer, i.e. at the time of delivery of the product, d) the reduced value of the product and how it was calculated.[41] In particular, the decrease in the value of the defective product is calculated on the basis of the proportional relation existing at the time of the passing of risk between the market value of the defective and non-defective goods.[42] The Supreme Court in its judgment 796/2015 has ruled that the buyer has to clarify all various types of defects on all types of products which were found to be defective and state the original market value and the value of the defective products in order to calculate the proportion in which the price will be reduced. The amount of expenses paid by the buyer in order to repair the defective products cannot substitute the value of the defective product. *F. The right to compensation:* "If the promised quality of the product is absent at the time the risk passes to the buyer, the buyer may instead of the usual remedies based on art. 540 CC, demand *compensation for non execution* of the contract or, in accumulation, demand compensation for the *damage not covered* by the exercise of the buyer's rights. The same applies in case of a defective product, *due to the seller's fault"* (543 alinea a and b CC). In addition, the prevailing opinion argues that in case of rescission, the buyer may ask for *compensation for non performance without having to prove lack of interest* in keeping the product.[43] The buyer can also replace or repair the product himself/herself and ask for compensation of the expenses in case that the buyer has refused to repair the product or failed to do so[44].

G. Tort liability (in conformity with art. 8 par. 1 of CSD): The Greek Courts accept the extracontractual (tort) liability of the seller in case of a material defect of lack of the promised quality if these are attributed to the wrongful conduct of the seller by which he intentionally seeks to produce, strengthen or maintain a misconception or impression on the buyer in relation to the lack of property or the existence of the defect, irrespective of whether such conduct consists of a representation of false facts as true or a concealment or a silence or incomplete communication of the true facts whose disclosure to the buyer who ignores them was imposed by the good faith or from the existing relationship between seller and buyer. This conduct is considered illegal according to article 914 CC on tort

[41] Judgment of the Supreme Court no 574/2001.

[42] Judgments of the Supreme Court 860/2014, 1442/2012, 1373/2010, 1468/1998, and 642/1992.

[43] Pouliadis Ath., The liability of the seller, 2003, p. 188, Valtoudis, A., Compensation of the Buyer for material defect, Efarmoges Astikou Dikaiou, 2010, p. 267 and Kornilakis, op.cit., p. 141 (in Greek).

[44] Kornilakis, op.cit., p. 123-124.

liability because the seller intentionaly causes damages to the buyer.[45] Claims arising from the contract may be accumulated with claims arising from tort liability and may be exercised at the same time, but they cannot overlap, since the satisfaction of one renders the other superfluous, unless the provisions on tort liability grants the buyer additional legal protection, not provided by the provisions on non-conformity.[46]

H. Exemption of the seller's liability: The seller is exempted from liability only in case that the *buyer was aware* of the lack of an agreed quality at the time that the contract was concluded (art. 537 CC). Grave negligence of the buyer is not necessary[47]. However, the Supreme Court of Greece has ruled that if the buyer participated in a pre-sale testing of the product (sea vessel) without stating any reservation, he is deprived of the possibility to claim his rights because of lack of an agreed quality of the engine reaching a certain speed[48].

I. Time limits: Greece does not impose the two months deadline that most states have[49]. The time for the buyer to notify the seller of the defect or the absence of the agreed quality is "reasonable". The usual time limit for prescription is two years for sale of goods (art. 5 par. 1 of the Directive 1999/44/EC) and five years for sale of real estate (art. 559 CC). The seller cannot invoke the time limit of 2 years if the *defect or promised quality* was hidden/concealed or not duly notified or deliberately silenced by the seller at the time when the risk passed to the buyer. In such fraudulous cases the usual prescription of 20 years applies (art. 557 CC). In addition, the buyer may exercise his/her rights when sued by the seller to pay the price even if the time limit has elapsed, only if he/she has notified the seller of the lack of conformity within the 2 year time limit (art. 558 CC). An attempt to repair the product by the seller interrupts the 2 year time limit only in respect of the specific defect until the seller repairs it.

[45] Judgment of the Court of Appeals of Thessaloniki, no 2256/2015.

[46] Judgments of the Supreme Court of Greece 1190/2007 and 737/2011, published at Chronika Idiotikou Dikaiou with observations by K. A. Christakakou 2012 p. 120.

[47] Before the transposition of the Directive 1999/44 in 2002, the Civil Code had provided that grave negligence of the buyer could result in the exemption of the seller's liability. See Christianopoulou, p. 43. The Directive 1999/44/EC provides that the buyer should not reasonably be unaware of the lack of conformity (art. 2 par.3).

[48] See judgment of the One Member Court of Appeals of Piraeus (maritime disputes) 769/2014.

[49] Art. 5 par. 2 of the Directive 1999/44/EC: Member States may provide that, in order to benefit from his rights, the consumer must inform the seller of the lack of conformity within a period of two months from the date on which he detected such lack of conformity. 16 member states have imposed this obligation, while Greece did not submit the rights of the consumer in such a short deadline. See Christianopoulou, op.cit., p. 38.

Question 1.2.2.

The aim of the proposed Directive on certain aspects concerning contracts for the supply of digital content (COM(2015)634) to fully harmonise the rules for the supply of digital content (DCD) presents pros and cons. Its advantages include that: a) it is a full harmonisation Directive with *specific rules adapted to the reality* of digital content sales while there is no relevant specific legislation in the majority of states except for the United Kingdom and the Netherlands[50]; b) it will not be confusing to consumers on the geographical source of their entertainment, networking or knowledge since it will apply in both domestic and cross-border contracts; c) it will extend the definition of "digital content" to cover digital services and for the first time will include contracts for cloud computing and social media; d) it will clarify the rights and obligations of the parties in case of non conformity of the digital content to the contract (art. 5); e) it will specific rules for the trader's right to modify digital content that is to be supplied over a period of time and the consumer's rights to terminate the contract if the consumer is not satisfied with the modification (art. 15).[51]

However there are certain problematic areas : a) the inclusion in its scope of the supply of digital content in exchange not for a price but for *data as counter-performance* in the form of personal data or any other data (art. 3) has triggered the request of the EU Council for an opinion by the European Data Protection Supervisor (EDPS). In his Opinion, dated 27 June 2017,[52] the EDPS warned that "personal data cannot be considered as a mere commodity" while the DCD will upset the "careful balance negotiated by the EU legislator on data protection rules" and will put at risk the coherence of the Digital Single Market;[53] b) the

[50] European Commission (2015d) p. 3.

[51] Beale, H. The future of European contract law in the light of the European Commission's proposals for Directives on digital content and online sales. IDP. Revista de Internet, Derecho y Política. 23:3-2015, p. 9.

[52] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. L119/1 (4 May 2016). In addition, the current Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. L201/37 (31 July 2002) will be repealed by the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, COM (2017) 10 final (Regulation on Privacy and Electronic Communications), 10 Jan 2017.

[53] Fryderyk Zoll, Personal Data as Remuneration in the Proposal for a Directive on Supply of Digital Content in Reiner Schulze / Dirk Staudenmayer / Sebastian Lohsse (eds), Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps – An Introduction, 2017.

retainment of data after the termination of the contract.[54] Though there is the right of the consumer to retain back his data which he has supplied or the trader has kept after the contract has been terminated (Art 13).

The Council of the European Union has already agreed in its common position for some flexibility taking into account the reactions of the national parliaments[55] and the member states. Therefore total harmonization will not be provided for a) the hierarchy of remedies (art. 12) which causes problems in certain states like Greece and b) time limits for seller's liability with minimum 2 years. The European Parliament will also make amendments during the legislative procedure so that the DCD will contain efficient rules for the Digital Single Market.

Question 1.2.3.

The scope of application of the proposed Directive on certain aspects concerning contracts for the online and other distance sales of goods in COM(2015)635 (hereafter referred as OSG proposal) is less broad than the scope of the 2011 CESL proposal. The draft OSG will *not* apply to Business to Business (B2B) transactions or Business to SMEs; to the sale of physical carriers such as DVDs and CDs incorporating digital content in such a way that the goods function only as a carrier of the digital content and to distance contracts for provision of services.[56]

Its scope covers only cross-border Business to Consumers (B2C) sales (art. 1 par. 1) and thus coincides partly with the Consumer Sales Directive 1999/44/EC (CSD) and the Consumer Rights Directive 2011/83/EU (CRD) which both cover online sales as well.[57] The only differentiation of the OSG proposal is that it will apply *exclusively* to online sales and distance contracts. Therefore, what is an online or distance sales contract is an essential criterion for the application of the draft OSG. According to Art 2 (7) of the draft OSG,[58] this concept requires an organised distance scheme with no simultaneous physical presence of seller

[54] Rolf H. Weber, Data Protection in the Termination of Contract in Reiner Schulze / Dirk Staudenmayer / Sebastian Lohsse (eds), Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps – An Introduction, 2017.

[55] E.g. the Dutch Eersten Kamer der Staten-Generaal, Opinion on the application of the Principles of Subsidiarity and Proportionality, ST 13742 2016 INT – 2015/0287 (OLP).

[56] However, it applies to goods like household appliances and toys where the digital content operates as an integral partof the goods (smart television sets). In addition, where a sale contract provides both for the sale of goods and the provision of services this Directive will apply only to the part relating to the sale of goods (mixed contracts). See European Parliament, summary of the proposal, p. 2.

[57] Smits, The New EU Proposal for Harmonised Rules for the Online Sales of Tangible Goods (COM (2015) 635): Conformity, Lack of Conformity and Remedies (February 12, 2016). European Parliament Committee on Legal and Parliamentary Affairs, briefing note PE 536.492, European Union Publications Office, February 2016; Maastricht European Private Law Institute Working Paper No. 2016/01. (2016a) p. 7.

[58] The provision duplicates the definition in Art. 2 par. 7 of CRD 2011/83.

and consumer and an exclusive use of one or more means of distance communication, including via internet, up to and including the time at which the contract is concluded until the contract is concluded. However, the consumer is unable to ascertain whether the offer he/she received is part of a broader scheme.[59] In addition, interpretation problems have already arisen with the implementation of the CRD which had included the same concept.[60]

The OSG Proposal provides for a full harmonisation of: the conformity criteria for the goods; the hierarchy of the remedies, available to consumers; the periods for the reversal of burden of proof, extended from six months to two years; and the "legal guarantee", i.e. consumer rights vis-à-vis the seller in the case of non-conformity of the goods which exists at the time of delivery;[61] the "commercial guarantee" which is, however, subject to minimum harmonisation only, as in the CSD.[62] The commercial guarantee is offered by the seller or the producer on a voluntary basis, above the standard set out by the legal guarantee, which must be legally binding and provide consumers with certain information.[63]

The European Commission itself declares that the new OSG rules is based on the minimum harmonisation rules of CSD 1999/44/EC.[64] In fact, the new OSG proposal is a new version of the CSD with certain amendments, added rights and clarifications,[65] which will apply uniformly to all Member States. In the words of Professor Beale,[66] the OSG proposal is a "CSD+". As a new version of the CSD, the OSG proposal does not change the criteria for establishing conformity with the contract and requirements for conformity of the goods, i.e. establishing whether the goods are "fit for purpose" and free of fault, as Art. 2 (2) of the CSD 1999/44/

[59] Smits, op. cit., p. 7.

[60] European Commission (2017) Evaluation, p. 6 where the European Commission found difficulties in interpreting some provisions such as "the notion of outside the 'business premises' in off-premises contracts (Art.2 par. 8), the distinction between a digital content contract and a contract for paid online services...".

[61] For the distinction between the legal guarantee and the commercial guarantee see European Commission (2007) Communication, on the implementation of Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees including analysis of the case for introducing direct producers' liability, COM(2007) 210 final, 24 April 2007, p. 6 and 9.

[62] Mańko, R. (2016) Contracts for Online and Other Distance Sales of Goods (February 16, 2016). PE 577.962, EPRS Legislation in Progress Briefing, p. 6. Preamble of the Draft OSG, par. 14.

[63] European Commission (2007) p. 9.

[64] European Commission, Communication, Proposal for a Directive of the European Parliament and of the Council "on certain aspects concerning contracts for the online and other distance sales of goods", COM(2015) 635, 2015/0288 (COD), Brussels, 9 Dec 2015, p. 3 and European Parliament, Summary Content, 2015/0288(COD) – 09/12/2015 Legislative proposal, p. 1.

[65] European Parliament, Summary Content, 2015/0288(COD) – 09/12/2015 Legislative proposal, p. 1.

[66] Beale (2016) p. 12.

EC provides. The OSG proposal follows also the innovative "hierarchy" introduced by the CSD on the remedies to be chosen by the consumer according to the principle of the primacy of *in natura* performance before the right of price reduction or termination (Art.3 par. 3 CSD). This hierarchy of remedies is not foreseen in the CISG[67] and is similar to the German rule on specific performance.[68] Such hierarchy has been accepted in many Member States following the adoption of the CSD[69], but not e.g. in Greece.

Clarifications of the consumer rights provided by CSD are given by the OSG proposal e.g. on the obligation of the seller to take back the replaced goods at the seller's own expense (Art.10 par. 1) and the non-obligation of the consumer to pay for any use made of the replaced goods prior to replacement (Art.10 par. 3)[70], except if it exceeds regular use and only up to the price originally paid.[71] This draft provision reflects also the case law of the Court of Justice of the European Union.[72] However, there are many doubts expressed for this consumer obligation by the European Economic and Social Committee Opinion[73] and by the European Commission in its 2017 evaluation of the CRD 2011/83/EC.[74]

The aim should be to strike a fair balance between the interests of the sellers and the consumers. On the one hand, the OSG proposal deteriorates consumer protection in many Member States which have enacted stricter measures due to the previous authorisation by CSD. It would be unfair to lower the standards and thus minimum harmonisation must be allowed in one or two very important issues, at least for some transition period. Instead of lowering the high protection of the consumer in those Member States, there could be less burdensome measures, according to the principle of proportionality (art. 5 par. 3 TEU). For example, *a data basis in the e-justice portal* of the European Commission could inform sellers of such national measures.

[67] See Christopoulou (2008) p. 411.

[68] Schulte-Nölke, Zoll, Charlton (2016) p. 16-17. Schmidt-Kessel M, Silkens E (2016) Breach of Contract. In: Plaza Penades J, Martines Velencoso L (eds), European perspectives on Common European Sales Law, Springer International, p. 132-133.

[69] ECC-NET, Summary of facts on the legal guaranty of conformity and commercial warranties. https://www.europe-consommateurs.eu/fileadmin/user_upload/eu-consommateurs/PDFs/PDF_EN/REPORT-_GUARANTEE/tableau_EN_Legal_commercial.pdf.

[70] Smits, op.cit., p. 6.

[71] Mańko, op.cit., 6.

[72] CJEU Case C-404/06, *Quelle AG v Bundesverband der Verbraucherzentralen und Verbraucherverbände,* ECR 2008, p. I-2685, ECLI:EU:C:2008:231.

[73] EESC Opinion, par. 4.2.5.10.

[74] European Commission (2017) Evaluation, p. 6: In CRD the Commission found that there were difficulties in interpreting some provisions such as "the calculation of the diminished value of goods in cases consumers exercise their right of withdrawal after having used the goods more than necessary to establish their nature, characteristics and functioning (Art. 14 par. 2)".

On the other hand, some of the draft provisions of the OSG proposal "raise consumer protection standards to an unjustified level", e.g. the extension of the period of reversal of the burden of proof in case of non-conformity from six months to two years or the right to terminate the contract even for minor defects[75] or the abolition of the Member States' discretion to oblige the consumer to notify the seller of the defect within two months after detecting it. These "counterbalance" provisions are not supported by consumer organisations and deteriorate the interests of the seller in an unjustified way. Therefore they should not be included in the final Directive.

Question 1.2.4.
It is a great advantage for the enforcement of consumer protection law that the draft DCD will oblige the Member States to grant rights to certain bodies to take action before the national courts, such as national bodies, consumer organisations, or professional organisations (art. 18). Concerning however the choice of the European Commission to proceed with separate Directives of total harmonization, this may bring a lot of fragmentation on consumer rules in the internal market since according to the type of the contract, similar but different rules will apply. For example, the OSG Proposal focuses on key rights and remedies that are already set out in CSD 1999/44/EC, but in a different way. The DCD proposal includes different time limits for the reversal of the burden of proof than other Directives (the Council has decided for one year instead of six months). Also the choice for total harmonization of certain rules of the OSG will deteriorate consumer protection in many Member States which have enacted stricter measures due to the previous authorisation by CSD. Flexibility must be allowed in one or two very important issues, at least for a transition period.[76]

Question 1.2.5.
The Directive 2005/29/EC on unfair commercial practices (hereafter UCPD) ensures the same level of protection to all consumers irrespective of the place of purchase or sale in the EU. As the European Commission has recognised, consumers may be protected from unfair commercial practices also in their dealings with online platforms.[77] Social networks are increasingly becoming platforms where traders can use the 'network effect' (with shares and likes) to their online

[75] Council of the European Union, Opinion of the Austrian Federal Council of 30 March 2016 (7758/16), p. 5.
[76] D. Anagnostopoulou, The Withdrawal of Common European Sales Law Proposal and the new European Commission Proposal on certain aspects concerning contracts for the online and other distance sales of goods, in Maren Heidermann, The formation of Commercial Contract, Springer, London 2017.
[77] Commission Staff Working Paper on 'Bringing e-commerce benefits to consumers'.

advertising. The European Commission promises to ensure that the new advertising models remain compliant with the UCPD, especially as regards 'hidden advertising' and product information.[78] In Greece, the UCPD 2005/29/EC has to be distinguished from the 1914 law on unfair competition[79]. In Greece there was such a case with a Greek platform "Airfasttickets" which caused the reaction of many e-travel platforms (pamediakopes.gr, viva.gr, airtickets.gr and travelplanet24.com) accusing the platform as infringing fair competition. Because since May 2014 its constant "aggressive" practice was to sell airtickets at a price, below cost even below taxes contrary to any business logic[80].

Directive 1993/13/EC seems also well adapted to the digital environment reinforced by Directive 2011/83/EU (hereafter CRD). The Greek government proposes to extend the scope of art. 2 of Consumer Protection Law 2251/1994 (which has transposed the Directive) on any contract which has not been individually negotiated between the parties. Thus, a small or very small enterprise which is considered the weaker party when it negotiates a contract with a larger firm, will be able to make use of the rights conferred by the provisions of the new art. and defend itself against a contract containing abusive general terms and conditions of trade.[81]

The Directive 2011/83/EC can be used for digital platforms[82] since it provides that traders can use online platforms to market their products and conclude contracts. In case the provider of the platform does not only share information but acts in the name of or on behalf of the trader, the platform must comply with the Directive.[83] In fact, the use of online platforms for auction purposes is not defined as "public auctions".[84] Online trading platforms providers have the obligation to make sure that information about other traders as content providers is duly displayed.[85]

[78] See First Report on the application of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') , COM(2013) 139, Brussels, 14.3.2013, par. . 4.3.8.

[79] M.Th. Marinos, The modernization of the law on unfair competition after the introducation of the Directive 2005/29/EC for illicit commercial practices and the judgments of the Supreme Court 1125/2011 and 991/2014, Elliniki Dikaiosyni 2015, p. 321 (in Greek).

[80] http://www.tovima.gr/finance/article/?aid=610431.

[81] http://www.capital.gr/oikonomia/3220682/upo-anamorfosi-o-n-2251-1994-gia-tin-prostasia-tou-katanaloti.

[82] Transposed in Greece by the Joint Ministerial Decision no KYA Z1-891/30.8.2013.

[83] See par. 20 of the Preamble and art. 2 (2) for the Directive. See European Commission, DG Justice Guidance Document concerning Directive 2011/83/EU, June 2014, p. 30-31.

[84] European Commission, op.cit. p. 12.

[85] European Commission, op.cit. p. 24.

Question 1.2.6.
In Greece, it seems there is not any action before national courts on the basis of consumer law against online providers' terms and conditions. No such information was traceable.

Question 1.2.7.
For the Greek legislator it would be necessary to expand the scope of the rules on Business to Consumers (B2C) to Business to Business (B2B) and Consumers to Consumers (C2C), since in Greece the CSD 1999/44/EC has the broadest scope possible in Greece including sales real property, medicinal equipment and professional machinery, rights, sale of an enterprise as a whole[86] etc. Therefore the rules of the Directive cover not only consumer sales (B2C), but also business sales (B2B) and even peer-to peer (C2C) sales and second-hand products. Regarding B2B transactions Greece is a member state of the Vienna Convention on International Sales of Goods, which is the regulatory model for CSD 1999/44/EC. However some member States have not signed the CISG (UK, Portugal and Malta).

Regarding C2C transactions, the same rules apply since Greece has used its discretion to submit the sale of "second-hand goods", e.g. used cars[87] to the same 2year deadline as new goods (art. 7 par, 1 b of the Directive).[88] According to the 2016 OECD report, the transposition of Directive 1999/44/EC into earlier legislation such as the Civil Code, especially for legal guarantees has the consequence that the relevant provisions apply not only to B2C but also B2B and between consumers («C2C»), which potentially hampers sales of C2C goods through e-commerce platforms, including second-hand goods, primarily sold through e-commerce platforms[89].Therefore, the OECD is of the opinion that consumers acting as sellers are not able to guarantee the conformity of the product.

1.3. Geo-blocking

Question 1.3.1.
There is an interlink between the proposed Regulation on Geo-blocking and Regulation 1215/2012 since if the trader is considered «directing activities to another Member State where the consumer has its domicile», any dispute will be dealt by the courts of the member state where the consumer is domiciled, thus creating more costs for the unwilling trader. The criteria for determining

[86] Judgment of the Court of Appeals of Athens 3778/2008.
[87] See for example Judgment of the Court of Appeal of Pireus no 45/2015.
[88] Christianopoulou, The rights of the buyer due to lack of conformity to the contract terms, 2010, p. 32.
[89] OECD, op.cit.

whether a trader is « directing activities in a member state » are not clear neither in art. 17 of the Brusssels 1a Regulation 1215/2012 nor in art. 6 of the Rome I Regulation 593/2008 for the applicable law. Some cases are clearly included under this concept, e.g. advertising or offers addressed to consumers of a certain state, or catalogues and emails sent to consumers of that state, or announcing national telephone numbers or evaluations from nationals of that state.[90] Other criteria, e.g. language or currency used from the trader's website, are not usually considered adequate per se to demonstrate the direction of trader's activity, except if they are different from the usual ones used in the trader's state. However, a conditio sine qua non is that the contract is concluded without however having to prove a causal link between the e.g the advertisement and the conclusion of the contract.[91]

In Greece 65% of the Greek online consumers choose Greek websites.[92] Greek consumers use websites that «direct their activities» to Greece like amazon.com, booking.com and use the Greek language accompanied by «index.el.html».

In order to clarify the situation, it would be advisable that the criteria would be more clear so that traders are confident about their obligations and rights especially since geo-blocking will be prohibited. Further assistance in interpretation of the concept could be used in case of traders that belong to a certain system of exclusive or selective distribution by considering «passive sales» as not «directing activities» since the prohibition of passive sales would constitute a serious infringement of competition rules on art. 101 and 102 TFEU.[93]

1.4. Collaborative economy (COM(2016)356)

Question 1.4.1.

In December 2016, Greece has adopted Law 4446/2016[94] in which it has defined sharing economy («oikonomia tou diamoirasmou») as "any model where digital platforms create an open market for the temporary use of goods or services that are often provided by individuals". The Law has defined also digital platforms

[90] Nikas N./Sachpekidou E., European Political Procedure, Commentary of the Articles of Regulation Brussels 1a 1215/2012, Sakkoulas Publishers, 2016, p. 296-298, referring inter alia to the judgments of the CJEU C-190/11, Muhlleitner (6.9.2012) and C-218/12, Emrek (17.10.2013) as well as the judgment of the Federal Court of Germany BGH 17.9.2008, IPRax 2009.258, which has also decided that it is not enough that the name e.g. of a laywer exists in a certain webpage, if the webpage is not his and the contract cannot be concluded via that webpage.

[91] Nikas N./Sachpekidou E., p. 297 referring to par. 24 of the Preamble of Regulation 1215/2012.

[92] See OECD observations referring to the survey of the Laboratory on E-commerce and Business of the Economic University of Pireus.

[93] See the analysis of the concepts of active and passive sales, N. Zevgolis, Vertical agreements and Competition, Sakkoulas Publishers, Athens-Thessaloniki 2012, p. 125-128.

[94] Official Journal (FEK) A' no 240 dated 22 December 2016.

as "electronic, bilateral or multilateral markets where two or more user groups communicate via an internet platform to facilitate a transaction between them" (art. 111 par. 1)[95].

In Greece, activities of shared economy exist especially in the tourist sector (e.g. Airbnb and homeaway for renting accommodation through internet or mobile), and the transport sector (e.g. Uber for taxi services, hopinside.com for sharing the same itinerary, Etsy for online market place etc.). Some platforms have been established by Greek companies such as EasyBike.gr (for renting bicycles), StayInAthens.com (accommodation of exchange students in Athens, jamjar.gr (for selling hand manufactured goods)[96] and Beattaxi (taxi services).

In such a situation, the Greek legislator has taken measures in order a) to establish clear boundaries between the *business* activity developed through the exploitation of small-scale tourist accommodation and the *occasional* exploitation by private individuals of real estate they own to increase their income; b) to ensure a minimum level of protection for users and third parties while ensuring the quality of the tourism in Greece; and c) to address the phenomena of "black economy" and tax evasion resulting from the absence of a regulatory framework[97]. This is why the tax authorities in Greece have paid particular attention in cross-checking the platforms and social media in collaboration with the Police Unit for Persecuting E-crime in order to discover tax evaders who post their announcements in digital platforms.[98] The measures taken are:

A. For tourist accommodation (Law 4446/2016 as amended by Laws 4472/2017 and 4487/2017): In the framework of sharing economy the Greek legislation regulates short-term lease *concluded through digital platforms for a specific period of less than one year.* In its definition of such accommodation, the law has included not only apartments and houses, but also any form of accommodation with structural and functional autonomy. However, in 2017 the law was amended in order to also include *rooms inside apartments and houses.*[99]

In order to confront tax evasion and regulate the current sharing economy activities in Greece[100], art. 83-84 of Law 4472/2017[101] have inserted art. 39 A in

[95] For further information see Galateia Kalouta, Sharing Economy, Digital platforms and national laws, Efarmoges Astikou Dikaiou 2016 p. 679.

[96] See http://www.newsbeast.gr/technology/arthro/800973/ta-mesa-enishusis-tou-sharing-economy.

[97] Informative note of the Minister of Deveropment, September 28, 2016.

[98] Savvaidou K., Challenges for modern tax authorities (in Greek), Union of Greek Legal Scholars E--Themis, 2006, p. 3 at 10.

[99] Art. 111 par. 1 case d as amended by Law 4472/2017.

[100] See Pomida at https://www.pomida.gr/touristikes_misthoseis.php.

[101] Law 4472/2017, published at Official Journal (FEK) A 74 dated 19.5.2017.Before that art. 111 was amended by article 36 of the Law 4465/2017 FEK A 47/4.4.2017.

the Income Tax Code[102]. It clarified the taxation of short-term rental income in the context of the sharing economy as regular income from immovable property for individuals, taxed by 15% up to 12.000 euros or 35% up from that amount to 35.000 euros[103] provided that the property is *rented furnished* without the provision of any service other than the provision of bed linen. Income received is exempt from VAT[104]. If any other services are provided, this income is taxed as derived from a *business activity (including VAT)*.[105]

Under law 4487/2017 proprietors were allowed to designate a manager for the short-term lease of their accommodation who can be either an individual (the proprietors or one of the proprietors, a lessee or a third party) or a legal person or any other entity. The manager uploads the information on the property in digital platforms and is responsible for the short-term lease[106]. For the moment, real estate brokers seem not to be prohibited in becoming property managers and in exploiting appartments in this way[107].

The new law has also abolished some of the pre-conditions for short-term lease in the context of the sharing economy such as the restriction on the area leased (at least 9 m^2 with natural ventilation and heating) and on the number of accomodations to be let per person.

These new rules deviate from the usual Greek legislation for tourist accommodation[108] and satisfy the mandatory requests of the Union of Hotel businesses for regulation of the sector[109], since the accommodation market was deregulated[110]. The new Greek legislation imposes the following obligations: a)The obligation

[102] Law 4172/2013, Official Journal (FEK) A 167 dated .2017. See Circulars of the Secretary of the Independent Authority for Public Revenue G. Pitselis, no ΠΟΛ.1069/23.3.2015 and ΠΟΛ 1112/2017.

[103] Or 45% for the excess of 35.000 euros according to the provisions of art. 39 and par. 4 of art. 40 of Law 4172/2013, as in force.

[104] Art. 111 par. 3 of Law 4446/2016.

[105] Art. 21 of Law 4172/2013.

[106] The owner of the property or the sub-tenant when assigning a third party to the management of his / her real estate for the purpose of short-term lease, has the obligation to submit a Real Estate Lease Information Declaration in which he / she will record the details of the property manager. In the event of failure to submit it, he / she shall be deemed to be the manager of the property (art. 111).

[107] See Deutsche Welle for a survey by Suddeutsche Zeitung on Airbnb (a-39999277).

[108] For touristic furnished accommodations see art. 1 par. 2 of Law 4276/2014 which must be of 40 m2 at least, as well art. 46 of Law 4179/2013.

[109] Chamber of Hotels in Greece, Sharing economy and the position of the hotel sector (2015) at http://www.grhotels.gr/GR/BussinessInfo/News/Lists/List/Attachments/592/Sharing_Economy_%CE%9E%CE%95%CE%95.pdf (in Greek).

[110] Indeed, the third Memorandum between Greece and the Lendors (IMF, European Commission and European Central Bank) has abolished law 4276/2014 (FEK A' 155) art. 2 par. 1 and law 2160/1993 (A' 118), art. 7 par. 2. Everybody could rent his house without any control and evading the earned income from tax authorities. See http://www.fortunegreece.com/article/nikiazete-to-spiti-sas-meso-airbnb--erchete-mitroo-ipochreotikis-engrafis.

of registration of each leased property by the property manager with the "Short Term Real Estate Registry" kept with the Independent Public Revenue Authority of Greece;[111] and b) the obligation that the registration number in the Short Term Residence Register must visibly accompany posting the availability of the property for short-term leasing on the digital platforms, as well as on any other medium. In case of violation, the Independent Public Revenue Authority may impose a penalty of 5000 euros to the property managers, who have to comply with the law within 15 days.

The Independent Public Revenue Authority may request from any digital platform operating in the sharing economy any information necessary for the identification of accommodation managers and property that they hosted. In addition, the Minister of Finance and Tourism and the Minister of Economy and Development have the authorization, by joint decision, to define:

a) the terms of cooperation of the Greek State with the digital platform are defined and b) the geographical areas, where restrictions for reasons related to the protection of housing sector on the short term rent will *not allow*: i) the short-term lease of more than two (2) properties per proprietor; and ii)The rental of each property to exceed ninety (90) days per calendar year and for islands of less than ten thousand (10,000) inhabitants sixty (60) days per calendar year. This rule on maximum duration of short-term lease will not apply in case that the total income of the lessor or the sub-tenant from real estate property does not exceed 12,000 euros during the tax year concerned.

Finally, the Government has announced its intention to impose a tax of 3% per transaction on a digital platform[112], something which seems to be in line with the proposals to be discussed at EU level by December 2017.[113]

B. For transport: Urban transport was highly regulated with rules on taxi vehicles, taxi drivers, taxi licences and tariffs[114]. Taxi drivers are professionals regulated by law and the relation with their customers is not an employment contract.[115] Cases where taxi drivers urged customers who waited for public buses on bus stops to choose them instead or private buses "stole" customers from taxi drivers were designated as illicit practices against public morals[116]. However, in

[111] In case of non-submission of Short term Residence Decalration, the manager will pay a fine equal to the double of the price appearing in the digital platform at the day of the control.

[112] http://www.fortunegreece.com/article/nikiazete-to-spiti-sas-meso-airbnb-erchete-mitroo-ipochreotikis-engrafis/

[113] http://www.fortunegreece.com/article/gallogermaniki-simmachia-enantion-airbnb-google-ke--amazon/, posted at 11.08.2017.

[114] See for example Opinion of the Legal Council of State no 266/2016, dated 20 October 2016.

[115] Judgment of the Council of State no 2771/2013.

[116] See for example judgment of the Supreme Court no 1125/2011, published at Chronika Idiotikou Dikaiou 2012 p. 304 and Armenopoulos 2012, p. 171.

the era of the Memoranda of Greece with the Troika and in particular since 2012, the public transport passenger cars are classified to a) taxis for public use (seats with taximeter) and b) passenger cars for public use – special lease with 6 to 9 seats without taximeter.[117]

In 2011, a Greek digital intermediary platform under the name of Beat (a former Taxibeat) started operating in Greece. It currently employs 8.000 drivers, reaching almost 1 million customers. The company has expanded to Peru and Chile and was bought out by Mytaxi (established in Germany and operated by Daimler) in February 2017.

The international digital plaform under the name of Uber was established in Athens in 2014 as UberTAXI and collaborated with licenced taxi drivers conforming with the tariff regulations imposed by the Ministry of Transport. Having to confront two already established opponents of Greek interests (Taxibeat and Taxiplon) Uber has changed its model. Since September 2015, drivers (not taxi drivers) are hired by licensed car rental companies that work with Uber or have a licence for car rental with a driver.

Question 1.4.2

On the basis of similar inquiries from other European Competition Authorities, in consultation with the European Commission as well, the Greek Commission for Competition has exempted the agreements of booking.com and expedia.com with their suppliers from free competition rules. These online platforms promised to modify their co-operation agreements with managers of hotels and appartments on a pan-European basis in order to allow greater flexibility when booking and pricing and when communicating with their clients. Therefore, the cooperating hotel businesses operating in Greece are allowed according to the amended agreement of cooperation with the platforms to: a) set different room rates and offer different terms and availability between online travel agents; b) offer lower prices and / or better terms to non-online channels (such as telephone reservations, or customers coming directly to the accommodation reception or reservations within closed user groups), provided that they will not publish or advertise online those prices; and c) make free promotions to all previous guests of their accommodation, even if they have closed their stay through the abovementioned online companies.[118]

The Competition Commission, after assessing the new modified contracts of these two online travel agency companies with cooperating hotel businesses

[117] Art. 82 of Law 4070/2012, Official Journal A' no 82.

[118] http://www.tanea.gr/news/economy/article/5277088/egkrithhkan-oi-oroi-synergasias-twn-booking--kai-expedia-me-ksenodoxeia/.

in Greece, considered that there are currently no grounds for further investigation.[119]

Question 1.4.3

In Greece there is no problem with market access requirements. As demonstrated by our answer to Q1.4.1. Service providers in the collaborative economy may easily operate since the Memoranda of Greece with the Troika of lendors and the complying legislation have opened all regulated professions. De-regulation was also the request of the OECD which provided us with the first «toolkit» for opening up the professions. In addition art. 113(3) of Law 4314/2014 allowed, at the request of the Consumer Ombudsman, the consumer's right of access to products and services as an individual right and, in particular, as an expression of the right to economic freedom, the right to free personality development and the right to equality. The confirmation came with the representation of the Independent Authority "Consumer Ombudsman" at the National Commission on Human Rights.

In September 2017 the Greek Ministry of Infrastructure, Transport and Networks has revealed its intention to submit a draft law to regulate the sector. Beat accused the Ministry that the Draft Law on Urban Transport will transform Beat from an intermediary platform to a public transport company, and will force drivers into a 3 year exclusive employment as the company claims for the citizens to sign a petition in its favour. In an interview, the Minister revealed that the sector of intermediaries including digital platforms must be regulated in collaboration with the European Commission, in order to request from foreign companies to have a seat and legal representative in Greece, supervision of their tax and social insurance coordinates, supervision of their transactions, tax payments, driver and vehicle controls etc.[120]

Question 1.4.4.

There is no information on legal challenges for consumer protection neither in Greek case law nor on the Consumer Ombudsman site. However, in Greece, sales law is the same for everybody and it applies also in sales C2C even for accomodation services (see question 1.2.). This means all have the rights and obligations (legal guarantee for 2 years) of the Consumer Sales Directive and its remedies. Greece has not opted out for used products, so the same rules apply on sales of used products between C2C.

[119] Commission of Competition, Bulletin of Press, 22 September 2015.

[120] Interview of the Minister Mr. Spirtzis to journalist Nikos Evangelatos on September 30, 2017, posted by the Ministry of Transport at http://www.yme.gr/?getwhat=7&tid=21&aid=5692&id=0.

Question 1.4.5.
In a peer-to-peer provision of services the provider of the underlying service qualifies as a trader according to Greek law under the following conditions : First, under the Consumer Sales Directive, the concept of 'seller' also covers a trader acting as an intermediary on behalf of a private individual if the trader has not duly informed the consumer of the fact that the owner of the goods sold is a private individual[121].

Second, in Greece, the law makes the differentiation between renting activity and business activity.

Question 1.4.6
The TaxiBeat platform uses an online selection and evaluation system for each professional driver using his/her photo with his/her consent. The Ministry of Transport has recently insinuated that this practice may be an infringement of data protection of the professional drivers that collaborate with the platform and may lead to an evaluation based on racist motives or motives based on sex discrimination. The Minister promised that a relevant question will be submitted to the Independent Authority for Data Protection in Greece.

2. Digital media

Question 2.1.
The Presidential Decree on Audiovisual Media Services No. 109 of 2010[122], in Article 2 (1) (b) literally transposes the definition of "programme" as set in Article 1 (1) (b) of AVMSD: "a set of moving images with or without sound constituting an individual item within a schedule or a catalogue established by a media service provider and the form and content of which are comparable to the form and content of television broadcasting. Examples of programmes include feature-length films, sports events, situation comedies, documentaries, children's programmes and original drama".

In Greece publishers of newspapers in printed form or online are subject to a specific regulation. Apart from that, neither the National Regulating Authority (National Council of Radio and Television) nor the Courts have dealt yet with the question, whether a broader definition of programme, covering the delivery of online audiovisual material through digital platforms, is to be applied. Furthermore the legal questions arising from the on line delivery of audiovisual content are open and require a specific regulation[123].

[121] Case C-149/15, Sabrina Wathelet v Garage Bietheres & Fils SPRL, 9 November 2016.
[122] Available in English in https://www.epra.org/articles/media-legislation#GREECE
[123] Kousouni-Pantazopoulou A., Hybrid-TV and its Regulation (in greek), Dikaio Meson Enimerosis & Epikoinonias 2014, p. 500.

Question 2.2.
Although Internet platforms may not be subject to the same rules as those followed by traditional broadcasters their serious impact on users justifies their falling under a certain number of duties. This extend of responsibility may not be seen as quite far-reaching, as long as it focuses only on content harmful to minors and hate speech. To this perspective Article 28a of the AVMSD Amendment Proposal requires from video-sharing platform providers to take appropriate measures against content harmful to minors and hate speech. Paragraph 2 of Article 28a of the AVMSD Amendment Proposal is expressly defining the "appropriate measures" and therefore is not primarily clashing with Articles 14 and 15 of the ECD.

A sector-specific rule is imposed to all ISS providers localized in Greece concerning on line gambling. According to Article 51 sec. 5 of Law No 4002/2011 on gambling services, ISS providers shall deny access to on line gambling providers not subject to a priori permission through the competent National Regulatory Authority (Hellenic Gaming Commission)[124].

Question 2.3.
No dispute regarding providers established in another Member State or outside the EU has been brought to the National Regulatory Authority (National Council of Radio and Television).

Question 2.4.
Ensuring the independence of NRA combined with the collaboration among European NRAs would facilitate the creation of a single market for audiovisual media services. Nevertheless the regulation regime governing traditional broadcasting services presents particularities. In Greece, electing the members of the competent NRA (National Council of Radio and Television) presupposes an agreement of the unanimity or the vast majority (4/5) of a special parliamentary body (Conference of Presidents) were all political parties of the Parliament are represented (Greek Constitution, Article 101A)[125]. This means that the NRA is not really independent and setting further independence requirements could clash with constitutional provisions.

In the years of economic crisis the Greek media market is going through a turbulent period of time starting with the sudden closure of the television ser-

[124] On the question of the compliance of this rule with the principal of net neutrality, see Kanellos L., Net neutrality: personal freedoms at stake?, (in greek), Nomiko Vima 2014, p. 816.
[125] This particularity (vast majority of 4/5 of deputies) has caused serious delays and problems to the efficiency of NRA, see Vlahopoulos S., Comment to the Decision No 95/2017 of the Council of State, Theoria & Praxi Dioikitikou Dikaiou 2017, p. 133. See also below under Q.3.4.

vices of the Greek public service broadcaster ERT[126]. In 2016 with a very controversial Ministerial Decision (No. 4297 of 1/3/2016) the Minister of State deprived the National Regulatory Authority (National Council of Radio and Television) from some of its competences[127], transferring them to the government (Secretariat General of Information and Communication)[128]. This transfer of competences came as a result to the impossibility of formatting a new Regulatory Body for a long period of time. The Supreme administrative Court with its decision No. 95/2017 of 13/1/2017 (Council of State, Plenary Session) annulled the Ministerial Decision stating that only the National Regulatory Authority (National Council of Radio and Television) is competent for the licensing of broadcasting services (Article 15 para. 2 Greek Constitution) and any transfer of these competences is a direct clash to the Constitution.

Question 2.5.

One of the most contentious issues in Greek broadcasting law has been the role of public service broadcasters[129]. The debate has initially focused on the lawfulness of their funding system based on a fee paid by all electricity consumers[130]. As in other countries the main issue on the independence of public service media remains active. Greek public broadcaster has always been accused of being a State broadcaster, tightly connected to the government.

To this perspective AVMS Directive could further proceed to the harmonization of legal measures guaranteeing editorial and journalistic independence. Apart from that it remains to Member States' initiative to implement all princi-

[126] IRIS – Yearbook 2013, Volume 1, The television market in Greece available in http://www.obs.coe.int/en. See also below under Q.2.5.

[127] These competences referred to the authority to license high definition, nationwide, free on air, DTT providers. See Economou A., Greece:Council of State decision on digital television licences, IRIS 2017-3:1/1, available in http://merlin.obs.coe.int/iris/2017/3/article19.en.html.

[128] European Regulators Group for Audiovisual Media Services (ERGA), 8th April 2016, Statement of the European Regulators Group for Audiovisual Media Services (ERGA) on alarming developments for the independent and effective functioning of media regulators in Europe, available in https://ec.europa.eu/digital-single-market/en/news/erga-statement-alarming-developments-independent-and-effective-functioning-media-regulators.

[129] On the most extreme act by the Greek government of closing down the public service broadcaster (ERT S.A.) in 2013, see Commissioner for Human Rights, "Public service broadcasting under threat in Europe", 2/5/2017, available in https://www.coe.int/en/web/commissioner/-/public-service-broadcasting-under-threat-in-europe. Economou A., Greece: Crisis over the Public Service Broadcaster, IRIS 2013-6/24, available in http://merlin.obs.coe.int/iris/2013/6/article24.en.html.

[130] Giannopoulos K., Comments to the decision No 2909/1988 of the Council of State (in Greek), Bulletin of Tax Law 1988, p. 1013. Mintzira K., The public broadcaster's fee (in Greek), Nomiko Vima 1995, p. 673. Theocharopoulos K., On the lawfulness of the public broadcaster's fee (in Greek), Bulletin of Tax Law 1991, p. 1651.

ples and standards contained in the recommendations of the Council of Europe on the independence and pluralism of media.

Question 2.6.
The Greek NRA (Hellenic Data Protection Authority – HDPA) has issued a range of Opinions and Guidelines referring to online targeted advertising and behavioral advertising[131]. No other initiatives have been referring targeted advertising on television. Targeted advertising presupposes collection of personal information about the user (e.g. gender, age, preferences). Although we don't see a need for an immediate EU-wide harmonization the effects of targeted advertising on privacy issues should be regularly reviewed and analyzed.

Question 2.7.
Greek Copyright Law (No. 2121 of 1993 as lastly amended with Law No 4481 of 2017, Article 54 para. 5) provides for a mandatory collective administration in case of retransmission through cable, whereas the relevant right can only be exercised by a collective administration organization. Similar rules have not yet been applied to online transmissions of broadcasting organizations, where the respective rights may be subject to collective administration on a contractual basis[132].

Question 2.8.
One of the main issues posed by cross-border portability is connected with the clearing of rights on an EU-wide scale. This problem aims to be solved by the New Portability Regulation[133] which simulates the temporary place of staying with the place of residence of the subscriber (Regulation 2017/1128 Article 3 sec. 1). In order not to turn to an infringement of legal interests of rightholders involved, cross-border portability requires a thorough verification of the subscriber's residence, so as to prove that it is a Member State resident and can enjoy the benefits of cross-border portability. This verification by the provider can be made by the conclusion of the contract[134] (which in any case is already occurring) and can be based on a minimum documentation proving its residence.

[131] Opinions and Guidelines of the HDPA available in http://www.dpa.gr/portal/.
[132] With webcasting by a broadcasting organization dealt the Civil Court of Athens (First Instance) in the cases No 7865/2002, 9332/2002, 8084/2009.
[133] Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14/6/2017 on cross-border portability of online content services in the internal market (OJ of 30/6/2017, L 168/1).
[134] So Regulation (EU) 2017/1128 Article 5 sec. 1.

3. Digital infrastructures

Question 3.1.

In April 2012 the Telecommunication Law No 4070/2012 ("Regulations of Electronic Communications, Transport, Public Works and other provisions", OGG Issue 82/A/10-4-2012) transposed European Directives 2009/140/EC and 2009/136/EC of the European Parliament and Council into Greek law. Article 3 paragraph 1 section γ, paragraph 2 section ζ introduced a rule on net neutrality, which repeats the rule of Article 1 paragraph 3a of the Framework Directive[135]

For the scope of net neutrality set in Article 3 paragraph 1 section γ of Law 4070/2012, objective, transparent, non discriminatory and proportionate regulatory measures shall apply, mainly through the respect of fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law when Measures shall be taken regarding end-users access' to, or use of, services and applications through electronic communications networks.

Any of these measures (regarding end-users' access to, or use of, services and applications through electronic communications networks) liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial protection and due process (Article 3 paragraph 2 section ζ subsection ζα of Law 4070/2012)[136].

These measures may only be taken with due respect for the principle of the presumption of innocence and the right to privacy. A prior, fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms. In any case the right to effective and timely judicial review shall be guaranteed to the person affected (Article 3 paragraph 2 section ζ subsection ζβ of Law 4070/2012).

[135] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ("Framework Directive") (OJ L 108, 24.4.2002, p. 33), as amended by Article 1 paragraph 1 section b of the Directive 2009/140/EC.

[136] It is questionable whether the restrictions posed to service providers in relation to provide access to internet gambling services by Law No 4002/2011 (Article 51 sec. 5) comply with the principle of net neutrality, Kanellos L., Net neutrality: personal freedoms at stake?, (in greek), Nomiko Vima 2014, p. 816. See also above under Q.2.2.

It is obvious that the net neutrality principle has rather the character of a general principle and abstract scope with no further enumeration of specific rights for internet users and obligations for internet providers and national regulatory authorities.

Zero – rating as one of the commercial practices mentioned in Article 3(2) of the Regulation 2015/2120[137] is not prohibited as long as it does not limit the exercise of end-users' rights laid down in Article 3(1)[138]. As long as zero rating is not applied for access to certain applications (application – agnostic offers) it could be considered as an acceptable commercial practice[139]. Zero rating practices *may create economic incentives to use an application instead of competing ones and may lead to circumstances where end-users' choice is materially reduced in prac*tice[140]. Furthermore it is being emphasized that *zero rating may be restricting for end users' free choice and privacy and may be harmful for the development of a competitive digital economy*[141].

In Greece there is no specific legal regulation or other act issued by the competent NRA (Hellenic Telecommunications & Post Commission) specifically handling with zero – rating practices. According to the general rules of competition law applying, companies with a dominant position may not adopt practices which reduce competition by forcing other companies to remain out of the market (Competition Law No 3959/2011 Article 2 sec. 2).

Question 3.2.

The goal for a further harmonization of telecommunication networks and services should resolve the problem of law and practice fragmentations between Member States. Perhaps a strengthening of the role of NRAs towards a consistent application of the rules could assist to this direction. Also privacy issues and end users' rights should be taken into account.

[137] REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25/11/2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union

[138] See BEREC, Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, August 2016, p.10.

[139] BEREC, op. cit. No 40-43

[140] NRAs when assessing such commercial practices should take into account the spirit of the Regulation 2015/2120, Recital 7 which requires intervention against agreements or commercial practices which, by reason of their scale, lead to situations where end-users' choice is materially reduced in practice. To this end, the assessment of agreements and commercial practices should, inter alia, take into account the respective market positions of those providers of internet access services, and of the providers of content, applications and services, that are involved. National regulatory and other competent authorities should be required, as part of their monitoring and enforcement function, to intervene when agreements or commercial practices would result in the undermining of the essence of the end-users' rights.

[141] https://creativecommons.ellak.gr/2016/07/15/3-imeres-apomenoun-zitiste-na-prostatefti-i--oudeterotita-tou-diadiktiou/

Apart from the general obligations and measures harmonizing Greek Law to the four telecommunication directives (framework Directive, authorization directive, access directive and universal service directive) no further special broadband measures have been adopted.

Question 3.3.
Legal issues have arisen from the spectrum management, particularly from the lawfulness of imposing restrictions to the spectrum user's rights to be granted. As a general rule, the number of spectrum's users rights granted may not be restricted unless it is necessary for the efficient use of spectrum (Telecommunication Law No 4070/2012, Article 23 sec. 1). The tasks and responsibilities connected with the procedure followed for an eventual spectrum's users' rights restriction are being allocated between the competent Minister and the NRA (Hellenic Telecommunications & Post Commission), whereas the law specifies the extent of tasks and competences awarded to each one of these two[142]. Furthermore the NRA (Hellenic Telecommunications & Post Commission) is the only competent for setting the starting price in a public auction[143].

Question 3.4.
The formation and functioning of NRAs are either regulated directly in the Constitution[144] or based on a legislative rule[145] mostly in conformity to European regulations. In case of NRAs which formation is foreseen in the Constitution, their members are elected with specific procedure which requires the unanimity or the vast majority (4/5) of a special parliamentary body (Conference of Presidents) were all political parties of the Parliament are represented (Greek Constitution, Article 101A)[146]. Due to political reasons the lack of the necessary

[142] Based on a study conducted by the European University Institute in Florence the Greek government decided to proceed to a public tender for licenses of digital television of national coverage and in high definition standards reducing the number of the available licenses to four, although the existing private television stations with national coverage are eight. For more details, see Economou A., Greece: Application of law on licensing of digital television under controversy, IRIS 2016-5:1/20, available in http://merlin.obs.coe.int/iris/2016/5/article20.en.html.

[143] Kondylis B., Competences on the fixation of starting prices in invitations to tender concerning spectrum user rights, Dikaio Meson Enimerosis & Epikoinonias 2016, p. 25.

[144] Hellenic Data Protection Authority (Constitution, Article 9A), National Council of Radio and Television (Constitution, Article 15 sec. 2), Hellenic Authority for Communication Security and Privacy (Constitution, Article 19 sec. 2), Supreme Council for Civil Personnel Selection (Constitution, Article 103 sec. 7).

[145] Hellenic Telecommunications & Post Commission, Hellenic Capital Market Commission, Regulatory Authority for Energy.

[146] Economou A., Greece: Application of law on licensing of digital television under controversy, IRIS 2016-5:1/20, available in http://merlin.obs.coe.int/iris/2016/5/article20.en.html. See also above under Q.2.4..

vast majority makes the replacement of old members and the formation of a new Regulatory Body quite problematic or even impossible for a long period of time[147].

This was the case of the NRA regulating the broadcasting market (National Council of Radio and Television) which in 2016 with Ministerial Decision No. 4297 of 1/3/2016 was partially deprived from its competences. The Ministerial Decision has been challenged and annulled by the Supreme Administrative Court[148].

The problem remaining is that the State is not ready to totally entrust NRAs and to accept their competence in regulatory areas of high interest.

4. Data in the digital economy

Question 4.1.

In Greece there is a specific Ministry for Digital Policy, Telecommunications and Media. The Ministry[149] includes the General Secretariat of Digital Policy consisting of: a) The Directorate of Strategic Planning, Standards and Evaluation (with the Unit of Digital Strategy on Big Data, cloud computing and Digital Platforms, b) The Directorate for Works of Public Sector and c) The Directorate for Cybersecurity: The latter comprises the Division for Coordination and Domain Names of the State which "collaborates with the relevant Ministries and the Independent and Regulatory Authorities for the direct incorporation of the General Data Protection Regulation 2016/679"[150]. The Ministry has launched a common framework for the National Digital Policy 2016-2021, in collaboration with organisations, like the Organisation of Open Technologies founded in Greece in 2008, and comprised of 30 Universities and Research centres in Greece.

B) In June 2016 the Ministry of Justice has established a Law Committee for the transposition of Directive 2016/680/EU and the examination of eventual legislative measures to be taken for the correct implementation of Regulation (EU) 679/2016[151]. The Committee consists of an IT Law professor (Ms L. Mitrou), a Public Prosecutor, Representatives of the Police and the Ministry of Justice, a lawyer and the Head of Auditors of the Independent Authority for Data Protection.

[147] Antonopoulos A., Questions of functioning and competence of NRAs (in greek), Theoria & Praxi Dioikitikou Dikaiou 2016, p. 16.

[148] For more details on this legal challenge see above under Q.2.6.

[149] According to the Presidential Decree no 82/2017published in the Official Journal (FEK) no A' 117 dated 10 August 2017.

[150] See article 15 of the Presidential decree.

[151] Ministerial Decision 43519, published at FEK B no 1913 dated 27 Ιουνίου 2016, p. 21427.

C) The Data Protection Authority staff and experts have participated in many conferences and seminars in order to raise public awareness in the public and private sector. So have done other associations[152].

Question 4.2.
How are businesses in your country adapting to the new requirements of the GDPR such as those related to consent, impact assessments, privacy by design and by default?

The private sector has launched many seminars on training the personnel on the Data Protection Officer tasks[153], such as taking the necessary safety measures and designing policies for data protection, to proceed to Privacy Impact Assessment, to design products and services taking into account privacy by default or privacy by design, to proceed to data breach notification within 72 hours, to implement an Incident Response Plan, and to award compensation of clients whose data have been infringed[154]. Awareness events are also organized in the pharmaceutical sector[155], the advertising sector etc.[156] In addition, there are new insurance packages to protect companies from cybersecurity threats[157].

Question 4.3.
In Greece a debate is developed in relation to Internet of Things (IoT) and especially the issues arising privacy and data protection[158]. The competent National Regulatory Authority (Hellenic Data Protection Authority – HDPA) has denied the use of wearable location tracking devices designated for children[159]. HDPA has particularly focused on the danger for the equilibrated development of children's personality: children may be convinced from their early youth that being watched by cameras and other smart devices for their own safety is a "normal thing". The use of location tracking devices may be used to children only for health reasons. It is for health treatment reasons that the HDPA has issued permissions[160] to various communities to use smart devices which are equipped with

[152] See for example G. Dellis, For an effective public protection of data: the «miraculous new world» of the Regulation (EU) 679/2016, published at Journal of Administrative Law 2017, p. 2.
[153] http://www.dpoacademy.gr/el/.
[154] See http://www.cyberinsurancequote.gr/news/to-proto-programma-gia-data-protection-officers--stin-ellada-dimioyrgithike-apo-tin-dpo-academy-kai-tin-nomiki-vivliothiki/.
[155] See "Pharma Transformation – Compliance in a Digital Era", http://www.eefam.gr/%CE%86%CF%81%CE%B8%CF%81%CE%B1/newsid510/83.
[156] See http://www.edee.gr/default.asp?pid=19&la=1&artid=587
[157] Cyber & Privacy Insurance Quote, available at http://www.cyberinsurancequote.gr/.
[158] Pantazopoulou-Koutnatzi, Internet of Things, Dikaio Meson Enimerosis & Epikoinonias 2014, p. 346.
[159] HDPA Decision 112/2012, available in www.dpa.gr.
[160] HDPA Permissions 1252/2013, 1316/2014 and 1328/2014, available in www.dpa.gr.

GSM and GPRS systems and are processing health data of the persons concerned. These smart devices are allowed to be used for social and health services offered from the communities to aged and handicapped people with their prior consent.

Question 4.4.

The Greek courts have ruled that photos or information posted on e.g. facebook, twitter or blogs without the consent of the subject constitute an illegal data file processing under the Directive 95/46/EC and the Greek law 2472/1997. For example:

a) The acts of uploading and posting photographs of two people by one of them *without the consent* of the other on websites (such as "Facebook") constitute two separate and distinct forms of illegal automated processing, in particular the "registration" and "dissemination" of personal data of the individuals to which the photograph relates, according to the definitions provided by art. 2(d) of the Greek law on data protection 2472/1997. The Court ordered the offender who posted the photographs in order to ridicule the other individuals to take herself down the photographs from Facebook.[161] Information uploaded on a blog *without the consent* of the subject constitutes a data file processed[162]. In its Decision 17/2016,[163] the Independent Data Protection Aufhority has ruled that although there is an exemption for domestic use of data in social networks, the mayor's website with more than 1000 contacts could not be exempted. The existence of a large number of contacts and the use of the website as a means of communicating with the citizens *goes beyond the exemption for domestic use*, making the mayor a controller having all the obligations laid down in art. 7 of Law 2472/1997 on Data Protection in Greece. Thus the Mayor cannot reveal personal data of a third-party (disability pension) without his / her consent. This illegal posting had to be erased by the Mayor in 5 days.

b) Information uploaded on the facebook on the individual's own initiative does not constitute a data file and is not covered by data protection. The general terms for the facebook platform make it clear that once an information or photograph is on the facebook platform *this is not a data file*[164].

c) A digital platform for social networking like «twitter» is a place where an «offence of personality via the press» may be committed by an individual

[161] Judgment of One Member Tribunal of Thessaloniki no 1024/2015, published at Elliniki Dikaiosyni 2015, p. 1456.

[162] Judgment of the One Member Court of Appeals of Thessaloniki 1960/2014 published at the «Law for Mass Media» 2015 p. 487.

[163] Published at "Law for Mass Media" 2016 p. 313.

[164] Judgment of the Court of Appeals of Athens no 175/2014, published at «Armenopoulos» 2014 p. 1740, and «Law of Mass Media» 2014 p. 379.

who must be punished (e.g. pecuniary compensation paid by the offender to the victim).[165]

d) On the extraterritorial effect of the Case Google v. Spain C 131/12: The Greek courts have respected the «extension» of international jurisdiction provided by the general terms of Facebook which appoint Ireland as the state for suing Facebook[166]. The Greek courts cannot decide on an application of provisional measures on data protection (e.g. when the users were last active) if the provisional order cannot be executed in Greece since the general terms of the contract have lawfully extended the international jurisidiction to Ireland.[167] The Greek Court thus did not apply the «main activity doctrine».[168]

2. The Independent Data Protection Authority of Greece has issued three Decisions on the «right to be forgotten». The Authority seems to be in favour of the argument that article 17 of the Regulation concerns the right to erasure and not the right to be forgotten. In a number of cases brought before the Authority that were against Google, it recognized, under certain conditions, the right to erasure from search engine results (delisting), but not from the source of the information.

a) Decision 82/2016: A former CEO of the Hellenic Defense Industry submitted seven requests to Google Inc. for the delisting from eighteen links because they adversely impacted his reputation and personality. Some links contained private personal information in relation to *criminal proceedings* against him and others containing *inaccurate information in relation to his portrayed membership* in a certain organization. Google Inc. accepted his request for delisting the links that referred to the CEO's alleged membership, something that was irrelevant to any misuse of public funds by the CEO or any other public aspect relating to his position, but rejected his request for delisting information on criminal proceedings, arguing that they contained information related to his status as a prominent public figure which the public had the right to know. The Greek Authority affirmed that he was indeed a prominent public figure and that the public had the right to be aware of the information related to his role as CEO. The Authority invoked the fact that *this information was published after public discussions in Parliament and review by relevant public authorities had taken place.*

[165] Judgment of the Three member Tribunal of Athens, no 1767/2015.

[166] Judgment of the One Member Tribunal of Athens, no 10053/2013, Armenopoulos 2013 p. 2421, with observations of A. Anthimos. Also published in Epitheorisi politikis dikonomias 2014 p. 503.

[167] Art. 23 and 31 of the Regulation (EC) 44/2001 (Brussels I) and CJEU Case C-391/95, Van Uden, 17.11.1998.

[168] However in the judgment of the Three Member Tribunal of Athens no 457/2016 (not provisional measures), Google was ordered to pay a compensation of 100.000 euros because of the «offense of personality» of a known businessman because of its omission to delete the copies of the files/webpages that included an offensive posting of an unknown blogger. This case is also mentioned in Q.1.1.

It is worth to note that the aforementioned delinking occurred in both google.com and google.gr search engines but only for individuals using those search engines from Greece. The delinking, thus, did not apply to users that were outside Greece (e.g. the USA where the claimant now permanently resided).[169]

b) Decision 83/2016: An obstetrician requested the deletion of a specific link of the blog «troktiko» in Google's search engine, which was the only link that referenced his conviction to six years in prison (with parole) and suspension of his medical license for a year on charges related to his illegal facilitation of adoption of babies for his own profit when searching for his name. The doctor argued that this was sensitive personal information, that the sentence referred to the Court of first instance and was thus inaccurate, as it was greatly reduced later by the Court of Appeals (second degree), and that the blog itself was inactive with no administrator, thus depriving him of the possibility to request removal of the information. Google Inc. rejected his claim, arguing that his occupation as a doctor placed him in the public sphere and that the information was not inaccurate, as he had been convicted at both first and second degree.

The Authority observed that the claimant (doctor), although not a public figure at first look, could be considered to belong *within the broader public sphere as a member of a regulated profession* under the criteria established by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (former article 29) and now European Data Protection Board under article 94 of the Regulation (EU) 2016/679. However, the Authority ruled that the information contained in the blog referred to the decision of the Court of first instance, rendered inaccurate by the fact that there had now been a newer decision by the higher Court of Appeals and notwithstanding the fact that he had been convicted in both courts. In addition, the fact that there was no administrator to take down the page considerably impaired the ability of the claimant to protect his interests, adversely impacting his private life. Therefore, the Authority ruled that Google's denial was not properly legally founded in accordance with the evaluation criteria established by the European Data Protection Board, and that Google, as the Data Processor, should immediately *delink the blog's information from its search engine*. Therefore the Greek Data Protection Authority makes a broad interpretation of the legal concept of public figure and includes also members of a regulated profession when acting as professionals.[170]

c) Decision 84/2016: In this case, the claimant (a woman) requested the erasure of links that connect here name to websites of pornographic content, argu-

[169] See Panagopoulou-Koutnatzi Fereniki, The evolution of the right to forget (or forget to forget), in Greek, in Efimerida Dioikitikou Dikaiou, 2016, p. 714-722.

[170] http://lawandtech.eu/2014/11/04/right-to-be-forgotten/

ing that this content was completely irrelevant with her person and was aimed at harming her reputation and defame her. Google initially denied to delink the above information, arguing that the websites were clearly not related to the claimant. The claimant brought the case before the Authority, and the Authority requested that Google re-examine the case and better justify its denial. Upon re-examination, Google eventually satisfied the request of the claimant, erasing the above links from the search engine. However, the claimant submitted supplementary documentation arguing that, despite the delinking, an unknown person continued to link her name with website of that kind, for which she had submitted another request to Google (without bringing forth relevant proof to the Authority), and, later, additional documentation that a new link had appeared for which she had not sent a request to Google yet. The Authority stipulated that the same process as the original complaint should be followed in similar cases and links, and in the case where the claimant had not contacted Google, it dismissed her complaint as not following proper administrative procedure (she should have first sent her claim to Google before contacting the Authority).

d) Minutes of Plenary Meeting of the Authority on 28 June 2016: In its Plenary Session, the Authority dismissed the claim of a man requesting the removal of a link from Google's search engine with the argument that it defamed his honor and personality. This claim cannot be evaluated by the Authority, and needs to be judged by the competent Courts. The Authority informed the claimant that the arguments involved in his claim cannot be examined by the Authority, and that he has the right to submit a new claim (to Google and, in case it is denied, to the Authority) on new grounds (e.g. violation of data protection legislation) other than what was included in his current claim.[171]

[171] F. Panagopoulou-Koutnatzi, The evolution of the right to be forgotten (about forgetting the forgotten?) in Greek.

HUNGARY

András Tóth • Anikó Grad-Gyenge • András Koltay
Tamás Klein • Johanna Ottlakán • Izabella Szoboszlai
Endre Győző Szabó • Balázs Bartóki-Gönczy

1. Internal Market and electronic commerce : Internet and e-commerce

1.1. Electronic Commerce, liability of Internet intermediaries

Question 1.1.1.
Court cases in this field are not published.

Question 1.1.2.
The CJEU's case law went forward in the direction defined by the L'Oréal v eBay case. In the GS Media case and the TPB v Ziggo case it made obvious that the editorial activity and the knowledge of infringing activities by the service provider shall be qualified as per se infringing activity and the safe harbour test cannot apply.

Question 1.1.3.
Notice and take down is a tool with an extremely limited effectivity because it does not make possible to contact the effective infringing person.

Hereby we mention some proposals which could complement the notice and take down:

- special rules on blocking access to infringing websites (DNS or IP address)
- seizure or blocking of the domain name of the infringing service
- filtering in line with the E-com directive and the Information Society directive
- filtering and restriction on the basis of the traffic
- introduction of a graduated response-system

Question 1.1.4.
EU law makes it possible for the law makers of member states to incorporate filtering and blocking into the means of the protection of rights by way of codification, even as part of a gradual system, where infringement can be observed and filtering and blocking are aimed against a given person.

Regulating the frame of blocking and filtering seems to be a possible way of involving service providers into the struggle against infringements even if the implementation of the principle of proportionality is doubtful.

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.
We have no direct experience in court proceedings regarding the remedies under the Consumer Sales and Guarantees Directive. The Consumer Sales and Guarantees Directive was implemented by means of civil law rules that does not fall to be applied during the procedure before the Hungarian Competition Authority (hereinafter: 'HCA').

The Legal Analysis Group (about the experience of initiating preliminary ruling procedures) of the Mansion summarized the experiences of the preliminary ruling procedures. The following statements can be presented based on that professional compilation.[1]

87 references for a preliminary ruling in the field of consumers' rights were submitted to the European Court of Justice by the Hungarian courts. The main aspects of these cases were focused on the Directive 93/13/EEC on unfair terms in consumer contracts.[2]

Question 1.2.2.
The proposal might be appropriate to achieve a genuine digital single market and it is to be supported as it has special regards on the high level of consumer protection.

Perhaps the enforcement rules of the Member States will determine the effectiveness of the regulation. Actually the general objective assumes efficient and detailed enforcement rules. The possibility of real and effective control on the digital content suppliers is elemental achieving the goals of the proposal.

[1] http://kuria-birosag.hu/sites/default/files/joggyak/az_europai_unio_joganak_alkalmazasa.pdf
[2] The relevant cases: C-302/04. Case Ynos, C-137/08. Case VB Pénzügyi Lízing, C-243/08. Case Pannon GSM, C-272/11. Case Banif Plus, C-397/11. Case Jőrös Erika kontra Aegon Magyarország Hitel Zrt., C-472/10. Case Invitel

It's important to emphasize that a high level of consumer protection is needed, as consumers should benefit from fully harmonised rights. When they will have clear rights receiving or accessing digital content from anywhere in the EU, it will increase their confidence in buying digital content.

The other important factor is that guarantees and rights should be protected and supported too when the digital content is not supplied for a price but in exchange for (personal and other) data provided by consumers. Digital content is often supplied not in exchange for a price but against counter-performance other than money i.e. by giving access to personal data or other data. Those specific business models apply in different forms in a considerable part of the market, so introducing a differentiation depending on the nature of the counter-performance would discriminate between different business models. The applicability of the rules of the directives should not depend on whether a price is paid for the specific digital content or not.

Question 1.2.3.

The full harmonization of the proposed Directive is basically appropriate to achieve the goals of the Directive.

The Digital Single Market strategy enables better access for consumers and businesses to the online goods and services across Europe (one of the three pillars). This circumstance certainly helps to achieve the digital single market if the existing consumer protection levels across Member States are not reduced at the same time. Therefore, it is to be welcomed that the rules will be tightened at certain points for example the extension of the reversal of the burden of proof to two years by aligning it with the legal guarantee period.

However, it should be noted that Member States have the competence to execute the define rules. This circumstance can undermine consumer confidence, since it will still not be possible to guarantee that a voluntarily non-performing business in some form accelerates compliance. Also, national courts may find it harder to take action against foreign-based businesses.

Question 1.2.4.

In the long run the harmonised rules will have confirming effect on the enforcement of EU consumer protection legislation. Anyway it's still important to emphasize that the cooperation between the Member States' competent authorities and the effective enforcements rules are the most essential.

The Regulation No. 2006/2004[3] on consumer protection cooperation underlines that each competent authority shall have the investigation and enforcement

[3] Regulation (EC) No. 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation).

powers necessary for the application of the Regulation and shall exercise them in conformity with national law. It means that in case of a reasonable suspicion of an intra-Community infringement the competent authority has to have the right to require the cessation or prohibition of any intra-Community infringement. The network of authorities responsible for enforcing EU consumer protection laws in the EU – and of course in the EEA – is called Consumer Protection Cooperation (CPC). CPC has the following operations:

- Any authority in a country where consumers' rights are being violated can ask its counterpart in the country where the trader is based to take action to stop this breach of law.[4]
- Any authority can exchange information – about intra-Community infringement.[5]
- Competent authorities with the Commission support can coordinate their approaches to applying consumer protection law so as to tackle widespread infringements.

This system is actually capable of implementing very effective cross-border cooperation. This has been proven also by the fact that there have been more than 100 requests for enforcement for each of the authorities over the years and the number of requests for information is high, too.

However, it should be emphasized that cross-border enforcement can be further strengthened in connecting with the digital sector. With the penetration of the digital sector the real borders disappear. In the light of this, it is important for any e-commerce company to be aware that it is not exempted from any infringement by the fact that its service is not provided in the territory of the Member State in which its conduct is being carried out. It is welcomed that COM(2015)635 will be included in the annex to the 2006/2004 protocol, so it can be the subject of CPCS cooperation.

However the cooperation and the above right are important in case of the national infringements, too.

According the Section 18 of the Act XLVII of 2008 on the Prohibition of Unfair Business-to-Consumer Commercial Practices, under special circumstances, provided that there is no other way to terminate the infringement, the competent authority has the right to order the outside contractor to execute the authority's resolution to eliminate the unfair commercial practice.

This provision responds on the E-Commerce Directive and the UPCD enforcement regulation providing that the administrative authorities should

[4] According to the Article 8 of the Regulation No. 2006/2004.

[5] According to the Article 6 and Article 7 of the Regulation No. 2006/2004.

be able to order the cessation of, or to institute appropriate legal proceedings for an order for the cessation of, unfair commercial practices.

Regarding the question of the limitations of the liability of intermediary service providers (outside contractor), the HCA had cases against online booking sites in 2013 and in 2014.

These sites were: www.szallas.hu[6], www.lealkudtuk.hu[7] which offered special offers including travel deals, www.booking.com[8] and www.agoda.com[9]. These cases have been terminated without finding any infringement but some of the findings of the decisions might be relevant to this issue.

In the case No. VJ/113/2013. the HCA pointed that though the website operator is considered a hosting provider its activity in that round is not merely a technical, automatic and passive in view of the followings:

- the operator promoted its service directly to the consumers,
- the operator sent newsletters to the consumers in which the offers were presented outside the portal,
- the operator in some cases had a directly contractual relationship,
- the operator was economically interested in selling the offers because he had commission after the selling.[10]

The HCA noted in relation to the E-Commerce Directive that the intermediary service provider's liability is limited to the intermediary's service activity. The service provider in point of the content what produces could be considered as a provider – and is responsible for the content as well.[11] This interpretation was also consistent with the objectives set out in the

E-Commerce Directive. No appeal has been received against the decision so no judicial review has been received.

It's important to underline that the E-Commerce Directive has the purpose of ensuring a high level of integration in the field of information society services. Anything that acts against the consumers trust obstructs this goal. That is why the enforcement and the question of liability are so essential. The narrower the scope of liability the bigger the probability that illegal content cannot be removed from an online platform.

Disparities in Member States' legislation and practice concerning liability of service providers acting as intermediaries might prevent the functioning of

[6] VJ/112/2013.
[7] VJ/113/2013.
[8] VJ/70/2014.
[9] VJ/93/2014.
[10] According to the point 121. of VJ/113-103/2013. decision
[11] According to the point 126. of VJ/113-103/2013. decision

the internal market. However it's hard to find the balance between the different interests and to set appropriate standards.

Anyway the exemptions from liability established in the Directive cover only cases where the activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored. Moreover, obtaining actual knowledge or awareness of illegal activities, the provider has to act expeditiously to remove or to disable access to the information concerned, and there is the possibility to regulate the obligations on national level in order to detect and prevent certain types of illegal activities.

Question 1.2.5.

The aforementioned EU consumer protection regulations are generally appropriate for achieving a high level of consumer protection in the European Union.

The Unfair Commercial Practices Directive 2005/29/EC has been implemented by the Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers. Since its entry into force, the wording/formulation of the act has kept uninterruptedly the possibility for prevent consumers from unfair commercial practices by the acting authority.

Most decisions of the HCA are based on the aforementioned legislations. It follows that despite the changing digital environment, this legislation is capable of filtering unfair commercial practices against consumers.

The rules of the Unfair Contract Terms Directive 1993/13/EC can be found in the Act V of 2013 on the Civil Code. This means that enforcing these rules is possible also by independent consumer demand.

It must be pointed that in relation of unfair contract terms some organizations have a right of action in the public interest. This topic is closely related to the next question so it will be discussed there.

The Hungarian Government's regulation[12] is referring to the Directive 2011/83/EC on Consumer Rights. The Directive seeks to achieve a high level of consumer protection through full harmonization. The rules are focused on the cross-border potential of distance selling and on digital selling.

The Hungarian legislation in force basically builds on the independent demand of consumers. This poses some risk as we have pointed out several times. In accordance with the Directive the Hungarian authorities are primarily able to examine the information requirements provided for in the Directive.

In itself one of the directives is not able to protect the consumer in their online relations, but the directives reinforce the influence of each other undeniably so they are capable of achieving the defence function.

[12] 45/2014. (II.26.) Korm. rendelet

Question 1.2.6.

Given that it would be almost impossible to collect individual consumer's cases spending we would focus primarily on well-known and published actions initiated by public organizations or NGOs.

A number of consumer (state) organizations have launched consumer protection actions before the national court in connection with the General Terms and Conditions of online service providers in recent years. One of the most active organizations was the National Consumer Protection Authority (its legal successor is the Ministry of National Development).

Here we would mention only the PPO case.

PPO (Pre Pay Online) was an internet based deposit portal primarily used to pay highway stickers and to upload mobile phone balances by registered consumers.

During the registration process on the site it was necessary to enter the credit card details.

Investech Ltd., the operator of PPO automatically charged its customers account on January 12, 2010 with an amount of HUF 2490 each. As a legal basis they referred to the modification of the General Terms and Conditions on January 1 which was only published on the PPO.hu website and the registered users were not notified in any other form. The essence of the change was that the consumers paid up for HUF 2490 for the free service until the modification and this amount was automatically recalled by the "recurring" method.

The National Consumer Protection Authority has brought an action in the public interest against PPO in April 2010.

The court found that the contractual terms did not become part of the contract and therefore the HUF 2490 amount was deducted without any contractual basis.

The court obliged the website operator to automatically refund the registration fee to the users.

The court ruled that the provision of the General Terms and Conditions in which the operator included the right to fully or partly modify the general terms and conditions is invalid to all the interested parties.

The HCA as one of the national competent authorities was involved in the implementation of Regulation (EC) No. 2006/2004 and it has the right to initiate proceedings in consumer protection cases.

In 2011 the HCA launched an action in the public interest in the Ingatlandepo case (Case No. VJ/122/2010.), which will be presented in the followings. [13]

[13] http://www.gvh.hu/sajtoszoba/sajtokozlemenyek/2012 es_sajtokozlemenyek/7596_hu_a_gvh_elso_kozerdeku_keresete.html

Www.ingatlandepo.com, www.ingatlanbazar.com and www.ingatlanbazar.net are real estate portals with real estate ads based on the same database. If a consumer posts an advertisement on one the websites, this advertisement will appear on the two other websites as well. The online advertising service was promoted as free but after the first 30 days it became a pay-service. The consumers had to pay for the service; they couldn't delete their advertisements until the full of the claim was settled (the amount grew until the deletion of the advertisement). The recovery procedure was threatening and vexatious.

The HCA investigated the activities of the operators and found that they worked out unfair commercial practices against consumers using the websites when:

- they ignored consumer complaints about their services,
- in the context of their commercial practices they ignored the judgment of the Court of Justice ruling on the invalidity of certain parts of the general contract terms applied by the undertakings operating the websites prior to 14 August 2009,
- consumers who wished to contact the advertisers on the websites have been informed in a deceptive manner about the availability of the advertisements on the websites,
- before the consumers put their advertisements on the webpages it was suspended that the searcher had a registration obligation too – without registration the searcher couldn't contact the advertiser in connection with the advertisement,
- they tried to force the consumers with an aggressive commercial practice to meet their demands on advertisements placed on the websites.

At the end of 2011, in the Ingatlandepo case the HCA filed a public interest action to the Budapest Metropolitan Court against Experient Enterteiment Ltd. and Weltimmo S.r.o in order to annul the unfair general terms applied by the undertakings. The Budapest Metropolitan Court ruled in its decision (made on 27 April 2012) that the sections of the General Terms of Business, which became part of the consumer contracts and the HCA found them objectionable, were null and void. Consequently, any party entering into a contract with the respondent undertakings would not be obliged to apply the nullified sections of the business terms.

Section 51/B of the Act CLV of 1997 on Consumer Protection declares that all final decisions adopted by any consumer protection authority, the HCA or the court having regard to serious infringements committed in connection with electronic commercial services shall be made public on the website of the ministry of the minister in charge of consumer protection.

According the relevant regulation, serious infringements are those where the webshop or other electronic commercial service provider

- does not inform its consumers about some relevant company data or terms before the contract,
- acts against the consumers' right of withdrawal,
- applies proven unfair contract terms.

Currently there are 31 decisions in the ministry's serious infringements database[14] but none of them is of the courts or of the HCA. In the listed cases firms misused their commitments and obligations connected to contractual information giving, complaint treating, right to withdrawal and terms of delivery.

Question 1.2.7.

The Hungarian law enforcement sets higher standards for the due foresight in the case of companies than for the average consumers.

Since it often occurs that the small and medium-sized companies face misleading business practices despite the expected high consciousness and prudence, it seems necessary to expand the scope of the rules on B2C to B2B commercial practices.

The Act XLVII of 2008 on the Prohibition of Unfair Business-to-Consumer Commercial Practices[15] is applicable only for communication targeted natural person consumers even if there might be companies (i.e. professional costumers) among the clients.

When the examined communication targets only professionals or companies the applicable provisions are in the Chapter III of the Act LVII of 1996 on the Prohibition of Unfair Trading Practices and Unfair Competition. The Hungarian Competition Act prohibits the unfair manipulation of business decisions.

In the assessment of the allegedly misleading business practices, the benchmark is the average trading party who is reasonably well-informed and reasonably observant and circumspect as can be expected in a particular situation.

Regarding online markets and services (among them especially the dual platforms and the social portals) the companies specially exposured to the potential misleading information are the advertisers (facing for example unverified market leader or exclusivity claims[16]) and the companies (webshops) seeking for consumer faith improving solutions (facing for example false reliability test claims[17]).

[14] http://jogsertowebaruhazak.kormany.hu/
[15] Implementing UCPD
[16] http://www.gvh.hu/dontesek/versenyhivatali_dontesek/dontesek_2016/vj_49_2016_33.html
[17] http://www.gvh.hu/dontesek/versenyhivatali_dontesek/dontesek_2015/vj_108_2015_44.html

In these cases the value of the offered services is connected to the consumer's choice and behavior, so a false or not verifiable claim might distort effectively the decisions of the businesses.

1.3. Geo-blocking

Question 1.3.1.

The proposed text of the geo-blocking regulation states that compliance with its rules should not affect the provisions of 1215/2012 of the European Parliament and of the Council law applicable to contractual obligations and on jurisdiction. According to our views this means that the rules set forth by the geo-blocking Regulation will not affect the results of the test that is used to determine jurisdiction in consumer contract related cases. The specific rules of Brussels I. Regulation regarding consumer contracts are only applicable to those cases, where there is an existing contract between the consumer and the trader. However we have to bear in mind that the aim of the Geo-blocking Regulation is to prevent unjustified discrimination based on domicile while it shall not intervene in the freedom to enter into contractual obligations, therefore its rules only facilitate the access to services and don't oblige the trader to make a direct offer nor enter into a contract.

In order to start the proceeding in front of the court of the Member State of the consumer's domicile or place of residence, the Brussels I. Regulation sets forth several other criteria to assess besides the existence of the contract, and the nature of the contract. Article 17 paragraph (1) point c) of the Brussels I. Regulation sets out a condition to start a procedure in the Member State of the consumer's domicile: the contract has to be concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State. The relevance from the Geo-blocking Regulation's point of view lies within the notion of a service targeting the domicile or place of residence of the consumer. The question is whether compliance with the rules of the Geo-blocking Regulation can be regarded as targeting another Member State with a service. According to our opinion, if the provider of the service – in compliance with the rules of the Geo-blocking Regulation – doesn't restrict the access to online interfaces, doesn't reroute the customers to another version of the online interface, and doesn't apply general access conditions, this doesn't mean that the trader aims to target the Member State in which a consumer has domicile. (This viewpoint is more prominent in the first reading text of the Regulation.)

In the online environment there are several websites that allow for directly entering into a contract, this however shall not mean that the activities of the provider target all those Member States in which the website is accessible. The

Brussels I Regulation doesn't have a definition for the notion of „activities directed to the Member State in which the consumer is domiciled" our opinion is that we ought to take a look at the case law of ECJ. The Court held in Pammer and Hotel Alpenhof cases that it's not enough to determine that the trader directs its activity to the Member State in which the consumer is domiciled to assess whether the activity of the trader – irrespective of his intention – de facto targets different Member States. A service can only be deemed directed to another Member State if it is the intention of the trader to turn to different Member State than the Member State of his head office. The Court named the websites, and the ads placed on websites as examples as it pointed out that the fact that the trader's website is available in other Member State doesn't necessarily mean that the trader's activity is directed towards that Member State. Further evidence shall be taken into consideration to conclude whether a trader's activity targets a Member State: it shall be assessed whether the trader has expressed clear intention to solicit the custom of that State's consumers.

Furthermore it shall be taken into consideration when assessing the target of a certain activity whether the trader has concluded a contract with advertising sales organizations or search engine providers which facilitate the easier access of customers of a Member States (or with other words it shall be examined whether the trader has taken steps to let the consumers of different Member States to get information on the offer). An other point to consider is whether the website permits consumers to use a different language or a different currency. (Pammer and Hotel Alpenhof, C-585/08. and C-144/09, EU:C:2010:740).

We believe that when determining the jurisdiction one shall continue to assess all the aspects of the case in question. Our opinion is that even with the Geo-blocking Regulation, simple compliance with the rules of the new Regulation that facilitate easier access to services, will not be enough to determine the jurisdiction.

1.4. Questions related to the collaborative economy

Question 1.4.1.

Airbnb and Uber were two most common collaborative economy businesses in Hungary. However, the Hungarian legislator clarified in 2016 that the existing rules related to the traditional taxi services are applicable to the platform based passenger transport services as well.[18] Otherwise, the Hungarian legislator extended the traditional taxi rules to the new technology based passenger transport services like Uber.

[18] See: Act LXXV of 2016.

As of 24 June 2016 9 penalties-points may be imposed on the driver in the case of provision unauthorized passenger transport service, and the repeated infringement will result in another 9 penalty-points, which automatically entails withdrawal of the driver's license for at least six months.[19] The vehicle used for the unauthorized passenger transport service may also be withdrawn for the first time for a period of six months and for three years in case of repeated infringement.[20] The transport authority may order the electronic communication service providers to block the platform temporary which does not comply with the requirements (asset collateral and license based on reliability and professional competence) for passenger transport organizer (dispatcher).[21] This can be ordered if the transport authority has already imposed fine on the dispatcher but it continued to provide its unauthorized activity.

The Hungarian Tax Authority made it clear in 2016 that the short-term accommodation services enabled by e.g. Airbnb are subject to notification to the competent local authority and the payment of several types of taxes (e.g. city tax). The private individuals providing private accommodation shall have the option to select itemized flat-rate taxation[22] and they are subject to invoicing obligation as well but they are exempted from VAT up to 8 million HUF.[23]

Question 1.4.2.

The taxi drivers were the most active and effective in lobbying among traditional services providers in order to reach the extension of the applicability of the traditional taxi-related rules to the new platform based passenger transport services. They raised unfair competition concerns rather than traditional ones. They argued that the Uber actually provides taxi services without complying with the legal expectations of them (e.g. licence, insurance, fixed local taxi tariffs) therefore the Uber enjoyed unfair competition advantages and they asked the regulator to enforce the taxi service related rules over the Uber-like services as well.

Question 1.4.3.

The short-term accommodation services enabled by e.g. Airbnb are subject to notification to the competent local authority in Hungary.

The taxi services are heavily regulated in Hungary and subject to authorization issued by Transport Authority according to a Governmental Decree.[24] The

[19] See: Act CXXVIII of 2000.
[20] See: Act XL of 2012 (Section 12/F. §)
[21] See: Act XL of 2012 (Section 12/A. §)
[22] See: Act CXVII of 1995 (Section 57/A. §)
[23] See: Act CXXXVII of 2007 (Section 189. §)
[24] 176/2015. (VII. 7.)

Transport Authority assess if the applicant's company and cars comply with the local rules on the provision of taxi services prior to authorisation. The authorisation refers to a specific geographical territory where the taxi service can be provided. The applicant must also show that it meets the following conditions in order to get authorisation:

- personal reliability
- professional competence
- financial capabilities (including insurance and asset collateral)
- compliance with the local rules as proved by the competent local authority

Question 1.4.4.
Several taxi companies have been sanctioned because of omitting the conditions under which the favorable advertised tariffs were applicable prior to fixing the taxi tariffs by local regulation.[25] Besides that few more consumer protection issues can be identified altough no closed investigations yet regarding the digital economy in Hungary: the service evalution made by the other consumers based on their past shopping expereiences bacame more and more important. Therefore the sharing economy's platorm providers must ensure that the evaluations are real and not only the positive ones are showed. The pricing to be paid by the consumers must be clearly indicated prior to placing the order (no hidden cost like clearing after use of the rented flat). The platform provider must also clearly indicate the goals and conditions of handling of personal data prior to get the user's acceptance on it if the platform provider collects personal data in connection with the provision of serives made it available to to consumer thorugh the platform.

Question 1.4.5.
According to the Hungarian rules trader shall mean any person engaged in trading activities[26]. According to the relevant law 'trading activities' shall mean retail and wholesale trading activities, and commercial agency activities.[27] Under the Hungarian rule implemented the UCP Directive (2005/29/EC) of the EU the provider peer-to-peer services regarded as a undertaking if it is acting for purposes relating to his business or profession.[28] Accordingly the definition of the undertaking is identical to the trader as defined by UCP Directive.

[25] Vj-4/2012; Vj-44/2012.
[26] Act CLXIV of 2005 section 2/11.
[27] Act CLXIV of 2005 section 2/9.
[28] Act XLVII of 2008 Section 2/a.

Question 1.4.6.
Ratings based on the past consumptions and quality labels are important tools to reduce the ex-post risk of the consumption and enhance the informed decision of the consumers and make the consumer's decision more reliable. Therefore it is very important that those tools be trustful and real. The quality labels should be based on objective evaluations or should make it clear that the user of trust mark just paid for it. Accordingly the consumer protection authority should secure that services providers do not apply the quality labels misleadingly and do not influence harmfully the evaluations (e.g. show only the positive ones or allow fake evaluations).

2. Digital Media

The cornerstones of Hungarian media regulations are Act CLXXXV of 2010 on Media Services and Mass Media (hereinafter: the *Media Act*) and Act CIV of 2010 on the Freedom of the Press and the Fundamental Rules of Media Content (hereinafter: the *Press Freedom Act*). The provisions of the AVMS Directive were implemented into the Hungarian legal regime by these two Acts. For the most part, the EU rules are included in the former legislation, and only to a lesser extent in the *Press Freedom Act*, such as with regard to the prohibition of hate speech and certain advertising-related rules. The scope of media regulations, in addition to media services (see the definition according to the AVMS Directive) also covers the printed and online press products.

Among the other relevant legislation, we should also mention Act CVIII of 2001 on certain issues of electronic commerce services and information society services (hereinafter: the *E-commerce Act*) which implemented the provisions of the E-commerce Directive in Hungary. The scope of this Act (at least in matters having importance for our purposes) concerns that segment of Internet content that is not covered by the media regulations. This segment includes the online content services that do not qualify as online press products or linear (streaming) or video on-demand media services available on the Internet.

Question 2.1.
1. Theoretical background of differentiating among the different service types
First of all, let us underline that the jurisprudence established following the entry into force on 1 January 2011 of the *Media Act* implementing (most of the rules of) the AVMS Directive in Hungary is fully compatible with the findings made in the above mentioned New Media Online case and so the judgement did not require the transformation of the official interpretation of the law.

Hungarian media regulations divide the media falling under its scope into two groups; media services (including linear and on-demand) and press products (printed or online). The definition of media services provided under point 40 of

Article 203 of the *Media Act* conforms to that of the AVMS Directive. Press products are within the scope of the regulations only if they meet the requirements set for media services: (1) a business service nature, (2) editorial responsibility, (3) the purpose of providing information, entertainment or education, and (4) providing the general public with content as the principal purpose (point 60 of Article 203 of the *Media Act*).

It is indeed a complex question, one that can only be answered properly with individual, case-by-case deliberation/assessment, when audio-visual content published within the framework of online press products or news portals qualifies as independent (on-demand) media service, and when only as an "illustration" connected to the content of the press product. As far as online press products are concerned, it is important to determine how far the editorial responsibility extends regarding the content accessible from the given website. The editorial decision and hence the responsibility entailed can be determined in the case of an online press product by the "editing" or "embedding" of the given content into the website.

Hence, if a press product contains moving images, such as a video accessible through a link, in addition to texts and still images, this may qualify as on-demand media service. However, the same press product should be interpreted in a different way if the video content appears on the website of the online press product as a quasi-auxiliary content supplementing the textual content, as part of the article. In this latter case, the text and the audio-visual content provided through a link, as an auxiliary content to the text, should be assessed in a unified manner and interpreted as media content published within an online press product.

In derogation from the above, if the catalogue of audio-visual content is available to the public within the framework of a service meeting the criteria of an on-demand media service, separately from the press product, of which none is connected to the written (textual) content, then it qualifies as an on-demand media service.

It should also be noted that the legislative bodies concerned have declared during the currently pending revision of the AVMS Directive that the audio-visual content embedded in online press products does not belong under the scope of the directive, and so it does not qualify as any (on-demand) media service (new Section 3c of the Preamble).

2. The Hungarian legal practice

One of the peculiarities of Hungarian media regulations is that the Media Council (the Authority) has "ceded" the supervisory powers over on-demand media services and press products, by exercising its right vested in it by the Media Act, to the self- and co-regulatory organisations (Article 190 of the Media Act).

Hence, as a rule of thumb, the above-mentioned sectoral professional organisations have the right to proceed in connection with the content published within the framework of these services. Currently, the Media Council has agreements in place with four such professional organisations. The service providers that are not affiliated to any of the professional organisations are an exception to this. The Authority exercises supervisory powers over them in compliance with the rules specified under the media regulations.

Below three cases will be presented. In the first case the co-regulatory organisation proceeded, whereas in the other two cases it was the Authority.

The service connected to the website of the online press product (index.hu) but accessible via a separate address (index.hu/video), made of the collection of exclusively audio-visual content, was classified as an on-demand media service by the co-regulatory organisation having competence to proceed in the concerned case, namely the *Association of Hungarian Content Providers*. The videos did not relate to certain specific articles, but could be considered as a catalogue of videos available separately from the textual content, via their own addresses, and they also met all the other criteria of a media service, hence the relevant rules of media regulation could be enforced against the video concerned, as a programme, that was the subject of the objection.

In the other two cases, the Media Council examined whether the articles published in the online press product and the videos embedded in them qualified as online press products or on-demand media services (decisions no. 62/2013. (I. 16.) and 33/2017. (I. 17.)). In these cases, the Authority found that since the videos served in both cases to supplement and illustrate the textual content, they should therefore be considered in conjunction with the textual elements, as press products. The audio-visual content should be interpreted in the same manner, even if it was produced by a different entity or if it is located on another website and can be accessed from the website of the press product only through a link.

Question 2.2.

1. Regulatory questions regarding video-sharing platform services

According to the current standing of the AVMS Directive amendment, the scope of the Directive would also in future cover video-sharing platform services, as long as the service concerned meets the requirements of the definition. The proposals made regarding the amendment indicate that social media services are also included under the notion of VPS, as long as they contain audio-visual content to a significant extent. To make the application of the regulations clearer and more predictable, it is welcome news that, with due consideration to the complex nature of social media, the legislator is trying to provide guidance in

order to clarify the definition of this service, by providing individual preamble paragraph(s) to that effect.

The extension of EU media regulation, or at least part of it, to include social media is completely justified bearing in mind the rapidly changing media consumption habits and the widespread use of social media, mainly among young people. The Directive also makes it clear that certain areas of social media need to be regulated, among other reasons, because social media have an increasing role in informing the public, sharing information, entertaining and, within the framework of these, publishing audio-visual content. Beyond this, it is an uncontested fact that social media are competing for the very same audience and income as radio and television media services, which have by now deserved to be called "traditional media". The creation and maintenance of the digital single market therefore unequivocally justifies uniform rules, or at least uniform minimum rules, being introduced for this new media type.

With due consideration of the above outlined impact social media has on the audience and the market participants it seems justified to impose on it rules which are at least similar to those imposed on media services as far as the field of content regulation is concerned. As a result, in addition to laying down comprehensive rules regarding the protection of minors, the growing tide of content inciting violence and acts of terrorism, as well as promoting discriminatory views, clearly justifies the facilitation of effective action on the part of the EU Member States to combat hate speech. Accordingly, the implementation of EU-level rules to prohibit hate speech on video-sharing platform services deserves full support.

With a view to certain consumer protection considerations, it seems a well-founded idea that the EU authorities should enforce certain commercial communication-related rules vis-á-vis these types of services as well. Referring back to the above outlined reasons, the transformation of media consumption and usage habits resulted in a growing proportion of advertising spend going to online media, and in particular to the social media segment. The enforcement of certain minimum regulations on advertising (including here, in addition to classic advertising, sponsorship and product placement as well) serves not only the interests of consumers but also the interests of economic operators active in the advertising market, by creating a predictable, fair and equal market situation for them. Since social media compete for the very same audience as traditional radio and television media services, and since forecasts show that the audience of the former media type is expected to grow continuously and rapidly, the establishment (and/or maintenance) of different regulatory environments for these segments, in terms of the advertising rules, may therefore have adverse consequences for the future.

2. The Hungarian legal regulations

The E-Commerce Act contains special requirements and rules governing online content falling outside the scope of the media regulations, primarily in the field of child protection. One of these rules requires that service providers can only publish information that may seriously damage the intellectual, psychological, moral or physical development of minors if a warning is published prior to the appearance of the information concerned on the subpage containing that information on the possible harm to minors and, furthermore, if identifiers are placed in the source code of the subpage. This latter requirement allows child protection filtering software to filter out harmful content and to make it inaccessible (Article 4/A of the *E-commerce Act*).

The above mentioned law specifies a unique form of law enforcement when, by extending the scope of applicability of the notice and take-down procedure, it allows that minors holding personality rights or their legal representatives have the option to take action to protect the personality rights of minors in an effective way, according to precisely regulated rules of procedure, prior to or instead of a civil action criminal proceedings. As a result of the procedure, similarly to copyright infringements, there is an opportunity to remove the content (information) violating the personality rights of the minor concerned (Article 13 (13)–(15) of the *E-commerce Act*).

Question 2.3.

As far as the media services accessible in the Hungarian media market but falling under foreign jurisdiction are concerned, according to the most recent data from Mavise, the database of television channels and companies of the European Union, 85 linear and 21 on-demand audiovisual media services target Hungary.

Since 2011, the Media Council has revealed nearly 40 alleged infringements related to the protection of minors against media service providers established abroad, most of which were reported to the Media Council by the public. (The Media Council regularly monitors and reviews the catalogue of programmes of media service providers airing programmes (most of which are subject to classification) in Hungary but falling under foreign jurisdiction – such as the FEM3, Viasat3, Viasat6, Film+, AXN, Cool, RTL II, Super TV2, PRO4 and Sorozat+ channels. In the course of an inspection, it investigates the rules of the country concerned related to the protection of minors and the Hungarian media law provisions and also compares these.) As for the applications filed in connection with such content, the Media Council has taken two approaches since 2011.

– On the one hand, as a rule of thumb, it has forwarded these notifications to the partner authority having jurisdiction based on the cooperation agreements concluded with the foreign regulatory authority. Based on the

request, from the partner authorities, on one occasion CNA, the Romanian media authority, declared an infringement and imposed certain sanctions as well, whereas the British Ofcom established the infringement without imposing any legal sanctions in a small number of cases. In the vast majority of cases, the partner authorities did not find the examined programmes to be infringing, based on the media law rules of the respective member state. As an example, in April 2011, the Hungarian authority presumed that two episodes of the reality programme titled *Éden Hotel,* aired on the Viasat3 channel, which is under British jurisdiction but also available on the territory of Hungary, were infringing child protection and product placement rules. At the same time, Ofcom held that the programmes were in compliance with the child protection rules of the Broadcasting Code issued by it, pursuant to the authorisation granted by law, and so in the end it did not establish any infringement in the given case. Additionally, these procedures are always preceded by extensive preparatory work, such as analysis of the programmes by the authority and translation of the inspection reports, and then follows the procedure conducted by the partner authority. As such, sometimes even a year can elapse between the date of the notification and the day when the fact of infringement is potentially established. An example of this is the current cooperation with the Luxembourgish partner authority. The Media Council forwarded the notifications, namely the inspection reports and their translations, made regarding the channels of CLT-UFA S.A., registered in Luxembourg and permanently named RTL II., Cool TV and Film+. These reports found that 15 programmes materially violated the provisions aimed at protecting minors or the interests of minors. The procedure of the Luxembourgish partner authority has been pending ever since, with no information sent to the Media Council on the outcome of the procedure so far; only a letter dated 12 October 2016, wherein the authority indicated that the inspection had been commenced and they had requested the position of the representatives of the concerned media service providers. And the contested programmes were aired in November and December 2015. Finally, we should also mention that unfortunately, in several cases the foreign authorities did not even respond to the requests made by the Media Council.

– The other type of procedure is conducted by the Media Council when a material and obvious infringement is detected. In these cases, a procedure subject to special conditions is conducted by the Media Council itself against the foreign media service provider, in line with Article 176 of the *Media Act* and in conformity with Paragraph (2) of Article 3 of the AVMS Directive. Experience shows that the expected result was not produced,

not even when the Media Council presumed the alleged material and obvious violation of mandatory rules aimed to protect minors, and when it established the fact of actual infringement as a result of the regulatory procedure. The complexity and stringent conditions and time-consuming nature of the procedures on the one hand, and the interpretation of the law by Hungarian judges on the other, can be mentioned as reasons for this latter situation. (As the court judgement made in a member state raised objections regarding the form of establishment of the first and second infringements, since it found the procedure conducted by the authority to be in violation of EU law, it therefore repealed them both. In this way, at the end, the consultation mechanism could not be started and no measures on the merits could be adopted either.

Question 2.4.

Hungary has been expressly supporting the EU level proposals attempting to impose independence requirements for media regulators right from the very first stages of these legislative processes, as the independence of the authorities and bodies supervising the media market and the transparency of their activities are essential preconditions of the freedom of the press and media pluralism. Besides, Hungary's support for the proposal advocating the independence of media regulators is obvious since already at this stage, the Hungarian legal environment meets, in all of its elements, the requirements specified in the proposals made in the course of the process aiming to amend the directive.

Although the official Hungarian position represented during the official negotiations held in connection with the revision of the Directive clearly supports the EU level imposition of minimum standards vis-á-vis the regulatory authorities and bodies, in certain regards it is nevertheless understandable that other, partly dissenting voices are also heard. In member states of the European Union, even if they agree in general that independent media regulators are necessary, the institutional system of public administration is a typical area that also involves constitutional grounds, which in turn belongs to the sphere of national sovereignty, and so certain member states, such as Germany and Austria, find the European Union's interference in these issues, at least to this extent, injurious. At the same time, if we also take into consideration the proposals put forward, it is clear that the authorities and bodies touch upon issues connected to the budgetary and judicial systems as well, and so in certain cases these would require serious structural interference on the part of the member states.

The respective provisions of the Hungarian media regulations meet all the requirements laid down in the text currently being negotiated in connection with amendment of the directive. As a result, if these amendments are adopted,

the Hungarian legal system should not undergo significant, let alone comprehensive, modifications. For instance, among other things, the Media Act requires the functional separation and independence of the body supervising the media market, that is the Media Council, from the Government and other organisations, including market participants, and also the predictable availability of the financial and human resources required to accomplish its tasks, the rules of electing members, the transparency of its activities, and the option of judicial review against its decisions (Articles 123–128 and 163–165 of the Media Act).

However, in addition to enforcing the fundamental rules affecting the operation of the authority responsible for supervising the media market, the measures made by the body in the course of exercising of the powers vested in it and during the application of the law, are just as significant. The possibility of excluding any pressure or attempts of unfair influence from political and market participants and the option of effective judicial review against possibly unlawful decisions can help create and maintain a developing media landscape utilising the advantages of the digital environment. Hence, besides fulfilling the independence requirements, it is at least as important to ensure actual independence, which can mostly be assessed in the light of the operation of the authority (body) and the exercise of its vested powers. To "measure" the latter on the basis of objective rules is quite a difficult endeavour.

Question 2.5.

First of all, the media regulations that entered into force in Hungary in 2011 resulted in significant changes in quite a lot of respects, compared to the provisions of the previous legislation. Content regulation was probably the area least affected by the change in the legal environment. This means that, in this respect, the participants of the media market have been pursuing their activities under a quite similar regulatory environment since 1996, the entry into force of the first media act (Act I of 1996 on radio and television). The conformity of the regulations with constitutional principles is verified by the fact that the Constitutional Court examined the regulations on several occasions (see for example Constitutional Court decisions no. 1006/B/2001, 46/2007. (VI. 27.), 1123/B/2005 and 165/2011. (XII. 20.)) and for the most part found the rules of these laws, mainly concerning content regulation, to be constitutional.

As far as the most contentious issues of media regulation are concerned, we should also note that the application of the law in practice by the authority and the courts, perfected over the previous two decades plus the above mentioned findings of the Constitutional Court, created a predictable environment for the service providers. At the same time, a significant part of the areas brought up in the question as examples (such as commercial communications, hate speech

and child protection, but also quota regulations) are found in the EU regulations as well. Below we wish to provide a non-exhaustive list of examples of the most common case types, highlighting among them the relevant points on which the (legal) disputes were focused.

1. Prohibition of hate speech

Pursuant to Article 17 of the *Press Freedom Act*, no media content can be published that may incite hatred against any nation, community, national, ethnic, linguistic or other minority or any majority, as well as any church or religious group, or which may discriminate against these groups. Experience from recent years shows that, on an annual basis, there are only some four or five cases when the above mentioned facts of the case are presumed. However, based on the decisions made following the regulatory procedures, only one or two infringements are established. The low number of these decisions declaring an infringement is due to the fact that, while very often extreme or possibly injurious expressions are considered by the concerned persons as infringing, this in itself may not however provide the grounds to enforce any sanctions. We should also note here that the authority has the right to investigate the enforcement of the prohibition of hate speech prescribed by law, not only in media services but also in press products (the latest of such decisions being decision no. 551/2016. (V. 17.) of the Media Council adopted in connection with media content of this kind).

2. Respect for human dignity

According to Article 14 of the *Press Freedom Act,* it is forbidden to publish any media content that violates human dignity. The most frequent debate concerning this prohibition defined under law originates from the aggrieved persons mixing up the institution of the protection of personality rights afforded by civil law and the protection of human dignity afforded under the media regulations. Media regulation is not an instrument for protecting rights that can be used simultaneously with the procedures applicable in the event of a violation of personality rights. Instead, it is intended to provide institutional protection for human rights, including the right to human dignity, i.e. it acts in the interest of the audience of the media, by ensuring that the audience is provided with media content that respects human rights (as well). If, therefore, a given piece of content merely violates personality rights, the media authority has no power to proceed.

3. Impartial news coverage

Based on the requirement of balanced coverage, media service providers are required to provide balanced coverage on issues that may be of interest to the general public in their programmes serving information and news published in their

linear media services (Article 13 of the *Press Freedom Act*). According to the regulations, media service providers are obliged to present the related, relevant and different opposing positions to the public in their information on current affairs. The reason for the contentious situations related to this requirement of the law is that complainants often start procedures on the grounds of lack of balanced coverage when no report is published regarding a certain event (the procedure can be commenced only upon request, based on the respective complaint). However, this would entail a disproportionate restriction of editorial freedom, therefore Article 13 of the *Press Freedom Act* cannot be interpreted in this way. It is also frequent that the given programme left out certain things the applicant expressed. However, the requirement of balanced coverage is not a tool for ensuring the opportunity of speech. It is not the person of the speaker but the publication of the expressed opinion that serves the enforcement of the audience's right to information.

4. Rules on advertising

The provisions of the media regulations governing commercial communications (Articles 23–36 of the *Media Act* and Article 20 of the *Press Freedom Act*) are among those provisions of law the infringements of which are revealed by the Media Council during its regulatory inspections. The most common causes of legal sanctions imposed by the authority are violation of the rules applicable to product placement (primarily unjustified emphasis or direct calls for purchase) and product support, and the prohibition of surreptitious advertising.

As far as the question of the possible further areas to be regulated by the AVMS Directive is concerned, we can state that it is hard to find new domains in the field of media regulation where harmonisation would be acceptable to all member states. The currently pending revision of the Directive also demonstrates that there is unequivocal consensus in terms of certain issues of content regulation (see the restriction of hate speech, for example), whereas in other matters, the fundamental differences rooted in the legal culture of the individual member states come to the surface vigorously and hence it is much more difficult to reach and adopt uniform regulations on these issues (such as the organisation of the media authority and the regulation of public service media).

For this very reason, in our opinion, the extension of the common regulatory scheme seems feasible only and exclusively regarding those subjects for which it is justified or even necessary in order to enforce uniform, EU level interests. As such, we should consider extending the material scope of the AVMS Directive to include the new service types. Initiatives regarding this have been made during the revision of the AVMS Directive by placing video-sharing platforms services or social media under the scope of the regulations, and the regulation of these may be harmonised even further. There are several new types of services

still available which compete for the same advertising revenue and in the same market as "traditional" media. However, they typically result in competitive disadvantage, with their services provided from outside Europe, primarily from the United States, for audiovisual services established within the European Union, the latter being forced to meet stringent EU rules. Into this category fall over-the-top services first and foremost, but also search engine services.

Question 2.6.

No legislative initiatives towards the regulation of targeted (or behavioural) advertising have been made so far in Hungary; however, the provisions of several pieces of legislation and codes of conduct within self-regulation are applicable in this area. At the same time, we need to underline that, with due consideration of the difficulties of law enforcement in the online space, the enforcement of rules governing targeted advertising is far from being effective.

As for the question, first of all we should emphasise that these kinds of advertisements specifically tailored to individuals can appear in television broadcasting only to a very limited extent. For media services organising their programmes into pre-defined programme schedules, only and exclusively virtual technologies may allow the use of advertisements tailored to the individual customer. Theoretically we cannot therefore exclude the possibility of these advertising techniques being applied in linear media services; however, this may take place typically in conjunction with Internet browsing, in the online space.

As far as the legal regulations are concerned, the *E-commerce Act* and the *Advertising Act* (Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities) contain requirements related to this subject matter. According to these laws, the targeted, tailored sending of these electronic advertisements can take place only subject to the prior, unequivocal and explicit consent of the customer, and provided that the option of free of charge and unlimited, immediate cancellation of sending advertisements is ensured to the customer concurrently (Article 14 of the *E-commerce Act)*.

Besides the legal regulations, it is primarily the code of conduct adopted by the actors of the advertising market (Hungarian Code of Advertising Ethics of 2015) that contain requirements regarding unsolicited and personally targeted digital advertisements and online behavioural advertising (Articles 29 and 31). The rules set forth by the Code are fundamentally supervised by the professional organisations working in the field of self-regulation, primarily by the *Advertising Self Regulatory Board*.

It means that in Hungary, according to the current standing of the regulatory background, the definition of the frameworks of online behavioural advertising and the enforcement of the related rules are primarily assigned to the professional

organisations encompassing the market participants. However this does not mean that general compliance with the applicable legal rules, in particular the effective privacy requirements, could be neglected.

Question 2.7.

Pursuant to Act LXXVI of 1999 on Copyrights (the *Copyright Act*), satellite broadcasting of a work is also considered as broadcasting if the broadcast programme can be directly received by the public. A programme that is broadcast by satellite is considered as a programme that can be directly received by the public if the programme signals are transmitted to the satellite under the responsibility and control of a radio or television organisation and then transmitted without interruption back to earth for public reception (see Article 26 (2) of the *Copyright Act*).

Broadcasting by satellite has the following additional characteristics, compared to the base case of communication to the public and broadcasting.

One of the key elements of the definition provided by law is the satellite technology (the programme-carrying signals sent from the Earth are aimed to the satellite, and the satellite in turn "spreads" the programme-carrying signals over the area covered by the satellite – the so-called footprint); the other is that the programme-carrying signals included in the broadcasting chain should still be receivable directly by the public (in the same way as in terrestrial broadcasting).

In the case of satellite broadcasting too, it is the broadcasting organisation itself that decides on the content of the broadcast programme, and its intention,, already at the time of transmitting the signals, comprises broadcasting to the audience, including the possibility of reception by the public. In this process, the satellite acts only as an extended antenna of the "original" transmitter.

In terms of copyright law, the broadcasting organisation is responsible for the entire satellite broadcast. However, this usage, at least in Europe, has the unique characteristic that the broadcasting organisation and the public to whom the organisation intends to secure accessibility are typically situated in the territory of different states.

Encrypted broadcasting qualifies as broadcasting to the audience as well. The *Copyright Act* makes it clear who is the user in this process and marks off this usage from the rule on the simultaneous retransmission of the work broadcast to the public. Encrypted broadcasting, such as "pay-tv" is also broadcasting, as long as a group of persons (anyone) who can already be considered "public" is able to decode it, such as using a device purchased from a trading network authorised by the broadcaster. Hence this is still "direct accessibility" (Article 26 (1) of the *Copyright Act*).

In this regard we should also refer to broadcasting to the public through cable or any other manner, as a method of use, which can be either making its

own programme available to the public directly by cable or in any other non-material way (except for uncontrolled/omnidirectional electromagnetic waves), or possibly the (re)broadcasting to the public of a programme, deferred in time, which has already been broadcast by someone else, made available via cable. It is characteristic of this method too, that the same programme content is received by the public simultaneously. The only difference from broadcasting is that here the signals are not carried by electromagnetic waves.

In connection with on-demand broadcasting to an interactive audience, we can say that the technical development (Internet penetration) and the new legal obligations of Hungary [Article 8 of the WIPO Copyright Contract and Article II (2) (c) (ii) of the Hungarian-American Contract and Article 3 (1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society] made it necessary to regulate expressly under the law this delimited, narrow case of broadcasting to the public. Here too, we are talking about usage of the work in a non-material way; securing direct access to members of a public far away from each other, in a way where a specific device is needed for the members of the public to transform the transmitted work-carrying signals in order to hear or see it. However, unlike in the other cases of broadcasting to the public, here such access is ensured, where the members of the public play an active, initiative role in the final stage of the process and they perceive a different content of the broadcasting and not concurrently ("public separated in time"). Members of the public have the option of choosing not only from the programmes compiled by the broadcaster, but also from individual works or excerpts.

Question 2.8.

Portability actually represents a problem only in terms of the non-downloaded content legally accessible in a given member state (typically transmitted to the audience by streaming) due to the limited scope of the licence of the service provider to broadcast the content to the public, which does not cover each and every country. The barriers to cross-border portability of online content services are mainly due to the fact that the right obtained to broadcast contents protected by copyright and/or related rights, such as audio-visual works, is bound to a regional license; furthermore, that the online service providers may decide to serve only certain markets.

The issue of portability is not only a copyright-related problem on the one hand; on the other hand it is not a feature characteristic of our country. As the European Parliament emphasised in its report of 9 December 2016 on the proposal on the Regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market,

the problems related to the cross-border portability of online content services are different regarding the different sectors. Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market allows the option of Pan-European licences or licences covering several territories in the field of the music industry; the Regulation prepared within the framework of the currently ongoing EU level copyright reform is trying to find a solution for the audio-visual industry, which is struggling with the predominance of exclusive regional licences.

3. Digital infrastructures

Question 3.1.

The Hungarian Government and the competent national regulatory authority (NMHH) were following the European Commission's wait-and-see approach what is to say that no ex ante regulation was adopted with regard to net neutrality (unlike in the Netherlands and Slovenia).

Concerning the Hungarian approach to zero rated offers, the Hungarian NRA has intervened among the first Member States in order to enforce the Regulation's dispositions. The NMHH investigated in December 2016 whether Hungarian Telekom's 'Unlimited TV & Film' option complied with the net neutrality rules. This option allowed unlimited access to the TV GO and HBO GO services for 24 hours without deducting any data traffic from the subscriber's package or reducing data speeds, which normally apply after a certain amount of traffic is used. As a result, NMHH has ordered Magyar Telekom to suspend any offer of zero-rated over-the-top (OTT) video services to its mobile subscribers.[29]

In January 2017, the NRA has ordered Telenor Hungary to suspend as well its zero rated offer since it has discriminated amongst certain type of contents (such as chat and social media services) and has also positively discriminated amongst specific services. According to NMHH, this commercial practice might lead the end-users to use the zero rated services to the detriment of the other competing online services which might distort the competition.[30]

Question 3.2.

1. EU-wide licensing scheme

The idea of EU-wide licensing scheme was raised by the European Commission in 2013, with special emphasis on the unification of spectrum assignment and

[29] http://english.nmhh.hu/article/172521/NMHH_decision_on_nondiscriminatory_Internet, (downloaded: 18/07/2017)

[30] http://nmhh.hu/cikk/172994/Ujabb_dontes_a_megkulonboztetestol_mentes_internetezesert, (downloaded: 18/07/2017)

on licensing (upon simple declaration) of electronic communications service providers.

As far as the "simple declaration" system is concerned, it is evident that there are inconsistencies between national schemes which are mostly related to the language used for notification, different notification forms, legal documents to be provided scarce availability of any online notification tool, etc. These are administrative burdens for cross-border operators. The implementation of a one-stop-shop system facilitating the cross border provision of services and the development of a common, harmonised and simplified notification format might reduce these burdens.

As far as the spectrum assignment is concerned, it is much more a difficult and sensitive question. The draft Regulation of the Commission, leaked in 2013, aimed to harmonise the design of assignment procedures by specifying the regulatory principles and criteria to be taken in account when establishing authorisation conditions and procedures for rights of use for radio spectrum. These provisions might considerably limit the independence and flexibility of Member States. First, it is a politically sensitive question since the income from the assignments, auctions "belongs" to the national budget. Secondly, a common system might not be justified from professional aspects neither; the need for different bands of spectrum varies from Member State to Member State according to various characteristics (use of Internet, demand of the service providers, etc.). Therefore, it might be reasonable to leave the spectrum assignment in the sole competence of the Member States.

2. Broadband measures initiatives

Almost 50 government institutions, companies, business chambers, universities, research institutes and professional and civic organisations have established – as a national initiative – in June 2017 the so-called "5G coalition" which aim to support the development of the next generation of mobile telecommunications technology in Hungary. The coalition's goals include drawing up a 5G development strategy, establishing a testing environment that gives Hungary a say in setting global 5G standards and becoming the first to adopt those standards from 2020.[31]

The Hungarian Government has launched the Digital Welfare program of which the "Super Fast Internet Program" is a sub-program. It aims to achieve that all households have access to 30Mbit/s Internet by the end of 2018,[32] i.e. 2 years prior to the deadline fixed by the European Commission (Digital Agenda 2020).

[31] https://dailynewshungary.com/hungary-establishing-coalition-support-5g-development/, (downloaded: 18/07/2017)

[32] http://www.kormany.hu/hu/miniszterelnoki-kabinetiroda/digitalis-jolet-program/szupergyors-internet-program, (downloaded: 18/07/2017)

Question 3.3.
The NMHH Regulation (7/2015) on the national spectrum assignment and on the rules of use is currently under the European Commission's notification procedure.

Although currently there are no specific on-going legal cases related to spectrum management, it is worthy to mention one issue related to this topic: shared spectrum use and its long-term effects on competition. The NMHH has approved in 2015 the agreement concluded by Magyar Telekom Nyrt. and Telenor Magyarország Zrt. on the secondary trading (lease) of the 800 MHz band obtained at the broadband frequency tender successfully completed in 2014. Secondary frequency trading receives priority support within the European Union as it considers one of the means to guarantee free competition in the communications market.[33] By sharing the spectrum, the two operators dispose over a much bigger amount of spectrum than their third concurrent, Vodafone Hungary. This might raise concerns from the operators not having such agreements. So it is not easy to find the balance between the efficient use of frequency and the efficient competition. Maybe the possibility of an effective ex ante regulation should be taken into account in order to avoid market failures due to these type of agreements.

Question 3.4.
No such (legal) issues have been raised in the recent two years.

4. Data in the digital economy

Question 4.1.
Preparations are carried out at various levels. The Supervisory Authority (NAIH) [34] plays an important role in this regard but preparations of data controllers and processors are also crucial regarding the exercise of data subjects' rights. NAIH meets representatives of data controllers and processors frequently and provides information on GDPR related implementation issues.

The first pieces of legislation concerning the implementation of the GDPR has been passed by the National Assembly, providing 30 new staff members[35] and related costs for NAIH. The Privacy Act of Hungary also needs to be amended significantly. Discussions are still ongoing and no draft has been tabled by the Government [36] so far.

[33] http://english.nmhh.hu/article/165939/NMHH_Approves_Interconnection_of_Magyar_Telekom_and_Telenor_Networks, (downloaded: 18/07/2017)
[34] National Authority for Data Protection and Freedom of Information, in Hungarian: Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH.
[35] In addition to the existing 75 staff members, which is a significant increase indeed.
[36] The draft will be published later in 2017.

Question 4.2.
The Authority does not have any official statistics about these issues. Despite the fact that the representatives of the Authority attend number of conferences and workshops, we have no direct information or formal feedback about how Hungarian stakeholders are adapting to new requirements of the GDPR.

At the same time, the Authority has some documents which could be useful for the data controllers to meet the requirements of the GDPR, such as the recommendations in general about the requirements of preliminary information of the data subject. The documents published by the European Commission are also useful in this regard and well received by interested parties. Guidelines issued by the Article 29 Data Protection Working Party also provide important input for data controllers.

It is also tangible that different stakeholders are interested in certifications and also drawing up code of conducts. The Authority encourages data controllers to consider this option.

It is a general feeling in the European Union that some businesses may not be prepared by the first day of the GDPR's applicability (25 May 2018), therefore targeted awareness programs might be required in the period to come.

Question 4.3.
The most contentious issues in Hungary in relation to IoT (Internet of Things) / smart cities / Machine-to-machine generated data / automated cars are determining the roles and liabilities of the stakeholders, data security, transparency and safety issues.

In many cases it is hard to distinguish the roles of the different stakeholders and point out who is the data controller or the data processor, in addition in many scenarios there are joint controllership which could blur the liability of the data controllers.

The data security issues are as severe, because these things and concepts are made with the mindset where efficiency overrides security issues. It is more important for an IoT device to have more battery power than to anonymize personal data. These concepts are also based on big and valuable databases / datasets which leads to information asymmetry and heavy profiling, in addition the stakeholders tend to hinder user control and transparency to be more effective.

There are many general data protection legislative measures which could be applied on these concepts. Also there is an overarching strategic document called the Digital Success Programme 2.0 which identifies all the major challenges of this area and fosters a policy debate between all the relevant stakeholders in this field.

Regarding the concepts of smart cities and intelligent transport systems further legislative measures are needed to mitigate the risks.

Question 4.4.

Hungary – as a Member State of the European Union – has implemented the Data Protection Directive of the EU into its national legal system. Hungary is also an active member of the Article 29 Data Protection Working Party. Furthermore, the judgments of Court of Justice of the European Union bind all Member States alike. Therefore, the legal status of the so-called "right to be forgotten" is the same in Hungary as in any other Member State. This means that under Hungarian law data subjects have the right to request the delisting of URLs that are excessive or no longer accurate or up-to-date.

The Authority has received 28 notifications since May 2014. These cases constitute the growing body of case-law. Although the Authority has no information on the relevant practice of the courts, data subjects may file for court action against the controllers in the event of any infringement of their rights.

The Authority follows the guidelines issued by the Article 29 Data Protection Working Party in order to strike a fair balance between the individual's right to data protection and other interest at stake.[37] The Authority has also published a guidance on the right to be forgotten concerning Google Search. The guidance which is available in Hungarian may be accessed via the website of the Authority.[38]

[37] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

[38] htpp://naih.hu/files/2015-07-29-Tajekoztato_Google_talalati_list_eltavol.pdf.

IRELAND

Florence Loric*
Jenny Mellerick
Claire Waterson

1. Internal Market and electronic commerce : Internet and e-commerce
1.1. Electronic Commerce, liability of Internet intermediaries

Question 1.1.1.
In the absence of a specific definition of "intermediaries" in the E-Commerce Regulations (European Communities (Directive 2000/31/EC) Regulations 2003) (SI No. 68 0f 2003), transposing the E-Commerce Directive, the Irish Courts have considered in some detail the activities undertaken by the Internet Service Providers to establish whether they can benefit from the liability exemptions under the Directive.

In *Mulvaney & Ors v The Sporting Exchange Ltd t/a Betfair* [2009] IEHC 133, the High Court considered whether Betfair, the provider of a betting exchange services on its website, betfair.com, could, in the context of comments posted on the chat room associated with its website, be considered to be an "intermediary service provider" providing a relevant service consisting of the storage of information provided by a recipient of the service for the purposes of reg. 18 of the Regulations of 2003. The plaintiffs argued that Betfair could not benefit from the liability exclusion on the basis that betting activities fell outside the scope of the E-Commerce Directive. Clarke J found that the relevant provisions of the directive and the relevant provisions of the implementing Regulations of 2003 were concerned with "activities" rather than the general business of the person

* All *rapporteurs* are from the Irish Society for European Law.

engaged in the activity concerned. While the general business of the defendant involved its facilitating betting, the relevant "activity" in the case was not betting in any sense of the word but rather the provision of a chat room and on the facts of the case, there was no significant nexus between the chat room activity, on the one hand, and the betting activity, on the other hand, which could reasonably lead to the characterisation of the chat room as being part of any betting activity that might be said to take place on the defendant's website. Betfair could accordingly rely on the intermediary defence to the extent that the provision of a chat room came within the meaning of provision of "a relevant service consisting of the storage of information provided by the recipient of the service" and it was an "intermediary service provider" within the meaning of the e-commerce directive.

Clarke J agreed with the broad interpretation given to the definition of intermediary service providers in *Bunt v Tilley* [2006] EWHC 407, [2007] 1 W.L.R. 1243, a case concerned libel proceedings against internet service providers, who, as intermediaries, provided a route to the internet which enabled third parties to pass electronic communications from one computer to another facilitating postings to a message board, hosted by other providers. Clarke J quoted the following paragraph of the judgment of Eady J: "*The claimant asserts that these defendants are not intermediary service providers. 'Simple logic dictates that to be an INTERMEDIARY service provider one must be a service provider who is BOTH customer of an upstream service provider and supplier to a downstream service provider'. Yet it is not a question of logic but of definition. No such restrictive definition appears in the regulations. Nor would it accord with the declared policy underlying them.*" Noting that there was no case law dealing directly with the question of whether the limitation on liability for hosting included the provision of chat room facilities, the Court noted that the E-Commerce Directive appeared to apply to chat rooms if they are hosting information provided by a recipient of the service and available to other users of the service. This was comforted by the report from the Commission to the European Parliament on the application of the E-Commerce Directive, stating, at para. 64, that "*In particular, the limitation on liability for hosting in Article 14 covers different scenarios in which third party content is stored, apart from the hosting of websites, for example, also bulletin boards or 'chat-rooms'.*" The Court concluded that Betfair was an "intermediary service provider" entitled to rely on liability exclusions (provided that the conditions of exclusion of liability were met).

In *Muwema v Facebook* 2016 [IEHC] 519, Binchy J in the High Court readily accepted that social media platform Facebook was an intermediary service provider.

A similar approach is taken in respect of the "*mere conduit*" exception. In *EMI v UPC* [2010] IEHC 377, Charleton J in the Irish High Court considered whether

UPC, an Internet Service Provider, was a "*mere conduit*" in the context illegal downloading of music files. On the evidence before him, Charleton J was satisfied that UPC was a mere conduit on the basis in particular that the there was "no modification of information in [the peer to peer] transmissions that is effected by UPC. Instead, the technical processes involved in stop and start, in terms of ordering the packets of information and their transmission, and their analysis by deep package inspection is not the modification or selection of any information." This was contrasted with "*tacking on an advertisement to a transmission, or modifying it so that some of it is lost, as opposed to being transmitted slowly*", which would have disabled the mere conduit defence.

Question 1.1.2.

Under the test for liability set out in *L'Oréal v e Bay,* a commercial service provider is not precluded from relying on the hosting defence, even where it has an economic interest in hosting material, unless it has control over, or forfeits its neutrality in relation to, the hosted content. In considering whether neutrality has been forfeited, *L'Oréal* supports a *"granular approach"*[1] so that the defence remains available in respect of services operated by the service provided including in circumstances where it is no longer available in respect of other services provided by the same operator. This approach resonates with the line followed by the Irish High Court in **Mulvaney** and is indicative of a reasonable test allowing to take into account the actual involvement of the ISP.

The "diligent economic operator" standard set in **L'Oréal** may not be quite as clear as regards the level of knowledge that will render a service provider ineligible for the defence, in particular in a defamation context. It has been noted that "*although this standard appears to be an intermediate one resting between actual and constructive knowledge, [bearing in mind that a standard of constructive knowledge may infringe Article 15 ECD] it has yet to be applied by Irish courts in the defamation context. The application of the "diligent economic operator" test therefore remains inherently uncertain under Irish law.*" [2] It should be noted in this regard that the question of whether receipt of a complaint for hosting defamatory content fixes service providers with actual knowledge, or awareness, is particularly complex in a defamation context, where at common law publication of a statement alleged to be defamatory is not *per se* unlawful if some recognised defence is available.

[1] Hugh J. McCarthy, "*Is The Writing on the Wall for Online Service Providers? Liability For Hosting Defamatory User-Generated Content Under European and Irish Law*", Hibernian Law Journal 2015, 14(1).
[2] Idem.

Question 1.1.3.

The regime of notice-and-take down regime set out by the E-Commerce Directive can be described as a compromise seeking to reconcile the effective protection of third parties' rights with the imposition of reasonable and proportionate obligations of intermediary service providers. As explained by the Irish Court of Appeal in *Sony Music Entertainment (Ireland) Ltd, Universal Music Ireland Ltd and Warner Music Ireland Ltd v UPC Communications Ireland Ltd*, [2015] IECA 338 (a case concerned with breach of copyright), ISPs are generally non-infringing entities (although there may of course be cases where an individual ISP is actually complicit in the infringement) and as a matter of traditional copyright law the mere fact that the facilities provided by a service provider are used for infringement purposes or even to facilitate an infringement does not in itself mean that such an entity is to be regarded as an infringer. The notice-and-take down regime exemplifies the trend towards increased responsibility for service providers in the Internet age and the need for novel solutions in the context where, as expressed by the Court of Appeal, "*the available evidence strongly suggest[s] that copyright infringement on the internet had become so ubiquitous that it posed an existential threat to the very fundamentals of copyright protection itself*".

The notice-and-take down regime does raise difficult questions for ISPs and courts as regards the removal of allegedly defamatory statements in circumstances where the ISP may have no means of knowing whether the allegedly defamatory statement is in fact true. In *Murewa v Facebook* [2016] IEHC 519 Binchy J in the High Court highlighted that a defamation case such as the one before him was very different from the circumstances of the *Sony* case but also cases such as *Tansey v Gill* [2012] IEHC 42 where the first named defendant was the author and publisher (on the Internet) of the defamatory material so that the Court had the benefit of being able to consider and receive evidence as to whether the defendant had a credible defence. Other issues may arise including the futility of take down orders in circumstances where the alleged defamatory statement may be published elsewhere. Different orders, such as *Norwich Pharmacal* orders, whereby the defendant, albeit an innocent party, is ordered to disclose information because a civil wrong is being, or was being, perpetrated against the plaintiff and the defendant, though not a party to the wrong, can identify the tortfeasor, may be appropriate and will allow proceedings to issue as appropriate against that person.

Question 1.1.4.

The Irish courts have considered a number of issues in respect of the granting of injunctions in the context of both copyright infringement and defamation cases. First, the Irish courts have dealt with a number of cases with their powers to

grant injunctions against non-infringing ISPs providing for "graduated response" notification systems and the nature of the remedy sought. In January 2009 the Irish Recorded Music Association settled an injunction claim against Eircom, the leading Irish ISP, Eircom having agreed to implement a graduated response, "three strike" scheme. In *EMI & Ors v UPC* [2010] IEHC 377, however, the High Court found that there was no jurisdiction to issue an injunction against an ISP requiring the prevention of infringements by subscribers, as Ireland had failed to transpose Article 8(3) of the Copyright Directive (Directive 2001/29/EC). On 29 February 2012, the European Union (Copyright and Related Rights) Regulations (SI No. 29 of 2 012) were adopted transposing Article 8(3) by introducing a new section, section 40(5A) in the Copyright and Related Rights Act 20000. The implications of section 40(5A) were considered in some detail in *Sony & Ors v UPC* by the High Court ([2015] IEHC 317 and [2016] IEHC 386), and on appeal by the Court of Appeal. The Court of Appeal upheld the order of the High Court granting an injunction requiring the defendant to operate a notification scheme at its own expense. This would consist of the sending of "cease and desist" letters by the ISP to its customers following the notification by the plaintiff of a detected infringement. After a third notification by the plaintiff, the ISP would disclose the fact that two notifications had already received, so enabling the plaintiff to apply for a *Norwich Pharmacal* order for disclosure of the identity of the account holder. The plaintiff would then be at liberty to seek an order under s. 40(5A) of the 2000 Act to suspend or terminate the account holder's access to the Internet. The number of notifications by the plaintiff would be limited to 2,500 per month.

Hogan J in the Court of Appeal considered the effect of Article 8(3) in circumstances where rightholders prior to the transposition of Article 8(3) were entitled to *apply* for an injunction against non-infringing ISPs. Hogan J found, having considered the caselaw of the Court of Justice of the European Union including in particular *L'Oréal, Scarlet Extended* and *UPC Telekabel Wien,* that Article 8(3) did not simply seek to fill a jurisdictional lacuna in the systems of civil procedure of the Member States by allowing rightholders to apply for an injunction against non-infringing ISPs. The caselaw of the CJEU confirmed that it was not simply procedural and it potentially changed substantive law by requiring Member States to provide their judicial systems with the authority to grant injunctions against non-infringing ISPs, subject only to certain safeguards (such as the prohibition against general monitoring of users). The Court of Appeal concluded that section 40(5A) "*empowered the High Court to grant an injunction in aid of rightholders against non-infringing ISPs but more fundamentally it gave the High Court the power for the first time to grant injunctions against persons and entities who themselves had committed no legal wrong and who had never threatened to do so*". This, in the words of Hogan J, "*represented a major change in the law, albeit in the relatively confined area of copyright*

infringement". It is in this context that Hogan J considered UPC's objections that the Graduated Response injunction was not of a kind normally granted by a court and was more akin to the type of order made by a regulator vested with specialist expertise. In this regard, "*once the legal Rubicon of vesting the High Court with a jurisdiction to grant an injunction against a non-infringing ISP has been crossed by the enactment of section 40(5A) of the 2000 Act, then what follows is really all merely a matter of degree*" and "*it could be said that any order made in those circumstances begins to take on the character of a regulatory solution*".

Having found that the effect of Article 8(3) was to permit the High Court to grant in principle injunction of the kind, Hogan J found that in the circumstances of the case, the order was necessary –the most obvious solution being in practical terms one which involves the rightholders informing the ISPs of the infringing activities of the latter's customers, with the ISP writing to its own customers about this conduct.

Hogan J also found that the order was not unnecessarily costly and complicated. There was no doubt that the solution required by the order would entail significant capital start-up costs together with ongoing operational costs. The only real technical solution was an automated solution which was of necessity complicated and costly. However it was not *unnecessarily* so.

In *Muwema v Facebook* [2016] IEHC 519, Binchy J in the High Court examined what remedies were available in respect of statements which were found to be defamatory (unless they were proven to be true). Although the normal remedy for defamation was damages, Binchy J noted that the application sought orders to take down the material already posted on the defendant's platform, to prevent the same activist to others from re-posting the same material and for *Norwich Pharmacal* relief. The Court examined the provisions of section 33 of the Defamation Act 2009 which provides that the Court may make an order prohibiting the publication of a statement if in the opinion of the Court it is defamatory and the defendant has no defence to the action that is reasonably likely to succeed.

Binchy J found that the jurisdiction of the Court was limited by the structures of section 33 and it was difficult to see "*at this remove*" "*how it could be said that the defendant is not reasonably likely to succeed*" having regard to the "*mere conduit*" defence available to it under section 27 of the Defamation Act 2009 as well as the hosting defence under the E-Commerce Regulations. Binchy J accordingly refused to grant the takedown and prior restraint orders although he granted a *Norwich Pharmacal* order. He admitted having come to this conclusion "*with some unease*" as, it appeared, "*a person who had been defamed by an internet posting may be left without remedy at all, unless the author is identified and amenable to the jurisdiction of the Court*". Furthermore, it appeared that the Defamation Act meant that victim could never obtain relief as against the ISP, which was shielded from it by being

a mere conduit and relief was not available under the E-Commerce Regulations as the Plaintiffs had contended. He concluded, "*if my concerns are well-founded, this is a matter of grave concern. Persons whose reputations are seriously damaged by anonymous abd untrue internet postings may be lef without any legal remedy against the site hosting the publication, even in the most flagrant of cases. The reluctance of the courts here and in other jurisdictions to grant prior restraint orders reflects the importance attached by the courts and society at large to freedom of expression. There must be a doubt however about whether an ISP, which disclaims any responsibility for or interest in the material complained about, is entitled to assert in defence of an application such as this, the right to freedom of expression of a party who has chosen to remain anonymous and remains at the time of the hearing of the application unidentified and beyond the jurisdiction of the Court and who in any event does not have a right to publish defamatory statements.*"

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.

The Consumer Sales and Guarantees Directive was implemented into Irish law by the European Communities (Certain Aspects of the Sale of Consumer Goods and Associated Guarantees) Regulations 2003 (the "*2003 Regulations*"). In the instance of a lack of conformity with a contract, in line with the Directive, the 2003 Regulations entitle a consumer to have the goods brought into conformity free of charge by repair or replacement, or an appropriate reduction made in the price or to have the contract rescinded with regard to these goods.

The legislative framework is over-complicated, as when transposing the Consumer Sales and Guarantees Directive into Irish law, it was decided not to integrate the new European rules into the pre-existing sale of goods framework, but instead to enact free-standing Regulations which operate in addition to the Sale of Goods Acts 1893. Pursuant to the 2003 Regulations, a consumer buyer of defective goods must elect whether to pursue his remedies under the provisions of the Sale of Goods Acts or the 2003 Regulations.

Furthermore the legal remedies available to consumers who purchases intangible digital content online are not clear. The Consumer Sales and Guarantees Directive defines "goods" as "any tangible moveable item", meaning that the protection afforded to consumers purchasing non-conforming goods does not extend to consumers purchasing defective digital content online.

Part 2 of the Scheme of the Consumer Rights Bill 2015[3] (which has not yet been enacted) aims to consolidate the remedies available under the Consumer

[3] Available at https://dbei.gov.ie/en/Consultations/Consultations-files/Scheme-of-a-proposed-Consumer-Rights-Bill-May-2015.pdf

Sales and Guarantees Directive with the rules relating to contracts for the sale of goods as contained in the Sale of Goods Act 1893 (as amended by the Sale of Goods and Supply of Services Act 1980). The provisions would clarify and strengthen the remedies available to consumers in cases of breach of contract, and would lessen some of the difficulties that have been faced in relation to the remedies in Ireland.

Question 1.2.2.
Addressing lack of clarity as regards contractual rights for faulty digital content (including music, movies, apps, games and cloud storage facilities) and available remedies is a key aspect of achieving a digital singe market.

Question 1.2.3.
While care should be taken to ensure that full harmonisation of key contractual rights does not reduce the level of protection effectively afforded to consumers, the harmonised treated of issues such as conformity with the contract, fit for purpose quality, delivery of accessories and replacement will contribute to achieving a genuine single market.

Question 1.2.4.
An appropriate measure of the effect of harmonisation would include increased consumers' confidence in purchasing cross-border and accordingly the level of growth of cross-border commerce.

Question 1.2.5.
Existing consumer protection law does not directly or at all deal with a number of issues which are to a large extent specific to dealings undertaken with or through online platforms including data protection aspect, consumer information in the context of reliance on algorithms and the level of protection afforded by consumer protection legislation in consumer to consumer trade undertaken though online platforms.

Question 1.2.6.
Here have been actions before Irish courts in relation to terms and conditions provided online through companies' websites. For example, *Ryanair Limited v Billigfluege* [2015] IESC 15 dealt with customers accessing the Ryanair website being automatically bound by the website's Terms of Use, which are provided in the footer of the site. However, there have not been any cases to date before Irish courts concerned with the terms and conditions of online providers.

Question 1.2.7.
It is not immediately apparent that all consumer protection rules should be extended to B2B commerce. Consideration may be given to an appropriate definition of consumers for the purpose of consumer protection regulation, including possibly the extension of the protection to SMEs (possibly on request).

1.3. Geo-blocking

Question 1.3.1.
The concept of "directing activities" has been considered by the Court of Justice of the European Union in a number of cases including C-255/08 *Pammer* and C-144/09 *Alpenhof.* Under the test adopted by the Court, all relevant elements must be taken into account in deciding whether a trader has directed activities to a Member State and evidence is required demonstrating that the trader was envisaging doing business with consumers domiciled in other Member States, including the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with those consumers. The Court dismissed suggestions distinguishing between websites enabling the trader to be contacted electronically, indeed even the contract to be concluded on line by means of an 'interactive' site, and websites not offering that possibility, a distinction according to which only the former are to be included in the category of sites that enable pursuit of an activity 'directed to' other Member States. The Court found that among the evidence establishing whether an activity is 'directed to' the Member State of the consumer's domicile are all clear expressions of the intention to solicit the custom of that State's consumers. It does not appear that the fact that a trader cannot use geo-blocking could be interpreted as an intention to direct its activities to all Member States for jurisdictional purposes.

1.4. Questions related to the collaborative economy

Question 1.4.1.
A key contentious issue arising in the context of the collaborative economy is the employment status, in terms in particular of employment v self-employment or independent contractor. The director general of the Workplace Relations Committee, Oonagh Buckley, has said that she anticipates that a collaborative economy worker will come forward in Ireland to have their working status decided "very soon".[4]

[4] High-level conference reveals mixed views on "gig economy" in Ireland, Andy Prendergast, I.R.N. 2017, 20, 25-26. Remarks made at Department of Jobs, Enterprise and Innovation "Future of Work" conference on 12 May 2017

In respect of Uber, current regulations in Ireland mean that Uber and other similar application-based services are restricted to only engaging licenced taxi drivers and chauffeur-driven cars. In the home delivery sector, Deliveroo has stated that riders seek flexibility and given the current legal framework in Ireland (of being either employed or self-employed), a more formal employment relationship with Deliveroo would not work for them.[5] Other issues include the application of planning law requirements to Airbnb. Share Economy Ireland, a non-profit industry association established in 2016 to advocate for those involved in the collaborative economy in Ireland and to establish standard for responsible sharing practices, includes among its members Airbnb, Deliveroo, Uber, and Stripe.[6] It is hoped that this organisation will work towards addressing issues which arise in respect of the application of existing regulation to new collaborative environments. Irish Congress of Trade Unions general secretary, Patricia King, has stated that the business model flourishing under the collaborative economy has implications for tax receipts, health and safety, workers' rights and social welfare receipts.[7]

Question 1.4.2.

The point is made from time to time that to the extent that new models of doing business operate on a different playing field, so that for example regulations (employment, health and safety etc) do not apply to them, they compete unfairly with traditional service providers. Many such issues, arising from disruptive new business models are issues which do not fall within the scope of competition law but rather concern the extent to which business and consumer protection requirements ought to apply to new service providers competing with traditional service providers.

There are a number of aspects which may then call for scrutiny under the competition rules. In particular if the new form of service involves the provision of services by individuals who are considered to be sole traders/self-employed or independent contractors, then the question of cooperation between competitors arise. For example taxi app's pricing systems, or so called "surge pricing", could raise competition issues in Ireland, along with how they utilise machine learning to calculate how much groups of customers will be willing to pay for a ride.

[5] High-level conference reveals mixed views on "gig economy" in Ireland, Andy Prendergast, I.R.N. 2017, 20, 25-26

[6] https://www.sharingeconomyireland.com

[7] High-level conference reveals mixed views on "gig economy" in Ireland, Andy Prendergast, I.R.N. 2017, 20, 25-26

Question 1.4.3.
Irish regulatory frameworks have largely not been modified to take into account service providers in the collaborative economy.

Airbnb itself has called for regulation of the home sharing sector in Ireland, with Patrick Robinson, the company's public policy director for the EMEA telling the Oireachtas Housing committee in June 2017 that unlike many other cities and countries in Europe, Ireland lacks an up-to-date regulatory framework that clearly recognises home sharing as a distinct short term rental activity.[8]

An Bord Pleanála (the Irish planning authority) upheld a ruling by Dublin City Council in 2016 that an apartment owner in Temple Bar needed to apply for planning permission if they wanted to continue to rent the property out via Airbnb.[9] A Bill which limits the time a person can rent his or her property on platforms such as Airbnb to six weeks has been drafted. It would also make it mandatory for all short-term letting companies to sign up to a register which will list all the properties they have on the books.[10]

Current regulations allow only licensed taxis to be booked through Uber, MyTaxi and similar apps, rather than private cars as is the case in other jurisdictions. The National Transport Authority have warned such providers that they must adhere to the provisions of the Taxi Regulation Act 2013.

Question 1.4.4.
Consumer protection issues reach the Irish courts from time to time. There has been significant amount of litigiation regarding whether or not a borrower is to be classified as a consumer for the purposes of the Consumer Credit Act 1995. *Stapleford Finance Limited V Peter Lavelle*[11] confirmed that there is no presumption or default position that a natural person is a consumer and that there is no requirement that such a definition be strictly interpreted.

Question 1.4.5.
There is no specific Irish legislation in respect of peer-to-peer provision of services. In order for a natural or legal person to qualify as a trader that person must

[8] Available at http://beta.oireachtas.ie/en/debates/debate/joint_committee_on_housing_planning_community_and_local_government/2017-06-28/3/. See Airbnb's submission to the Joint Committee at http://www.oireachtas.ie/parliament/media/committees/housingplanningandlocalgovernment/Airbnb-Submission-to-Joint-Committe-on-HPCLG-(Corrected).pdf

[9] http://www.irishtimes.com/news/consumer/temple-bar-airbnb-apartment-needs-planning-permission-1.2672246?mode=sample&auth-failed=1&pw-origin=https%3A%2F%2Fwww.irishtimes.com%2Fnews%2Fconsumer%2Ftemple-bar-airbnb-apartment-needs-planning-permission-1.2672246

[10] http://www.thejournal.ie/airbnb-bill-3459779-Jun2017/ and mentioned in Dáil Debates on 6 July 2017 at https://www.kildarestreet.com/debate/?id=2017-07-06a.14.

[11] [2016] IEHC 385

be acting for purposes related to that person's trade, business or profession or on behalf of such a person (Consumer Protection Act 2007, Sale of Goods and Supply of Services Act 1980). Provided tha when providing a peer-to-peer service a person is acting for purposes related to his trade, he will be considered to be a trader.

Question 1.4.6.
Online rating, review systems and quality labels can be appropriate tools to overcome the lack of information about individual service providers. However, such systems would have to be sensitive to the relevant regulatory environment and circumstance specific.

2. Digital media

Question 2.1.
The AVMS Directive was implemented into Irish law by the Broadcasting Act 2009 (the "**2009 Act**") and Statutory Instrument (S.I.) No. 258 of 2010, the European Communities (Audiovisual Media Services) Regulations 2010 (the "**2010 Regulations**"). It is also given effect through the codes and decisions of the Broadcasting Authority of Ireland ("**BAI**").

The definition of "programme" as interpreted by the CJEU in *New Media Online* is mirrored in Irish legislation, specifically Regulation 2 of the 2010 Regulations. Consequently, in principle, the Irish legislation bears the same interpretation without the need for amendment. The matter has not, however, been tested to date before the Irish Courts. Furthermore, there is no published decisional practice by the BAI on the concept of "programme".

Question 2.2.
Under the new proposal, among other proposed changes, video sharing platforms would be required to put age verification or parental controls in place with the aim of protecting minors from mature or inappropriate content. The proposal will also allow Member States to impose fines for non-compliance, if national legislation allows.

Any legislative moves which go towards enhancing the protection of minors and the combatting of hate speech can only be regarded as a step in the right direction. It would be difficult to argue otherwise. The application of rules regarding, *inter alia*, commercial communications such as product placement, sponsorship and advertising, may also be a step in the right direction. Clearly, the increased use of video platforms is likely to result in increased susceptibility to some potentially harmful effects of such communications. That said, the appro-

priate balance should be struck between protecting those potentially affected and imposing excessive regulation.

Currently, Ireland has limited sector-specific regulation in the audio-visual sector. The 2009 Act protects minors in relation to broadcasting services; however, a ''broadcasting service" does not include other audio and audio-visual services provided by way of the internet. In addition, films and video/DVD recordings are subject to classification by the Director of Film Classification, and may be prohibited or made subject to restrictions in certain circumstances (i.e., where they are unfit for general exhibition to the public by reason of their being indecent, obscene, likely to incite hatred, etc.). However, beyond this, Irish legislation does not contain sector-specific rules in relation to audio-visual platforms, but future developments along this line may be necessary. In particular, given the technological and social media developments since the AVMS Directive was introduced, it is necessary to look at different platforms and the extension of the scope of the Directive to protect minors and prevent hate speech. While there does not appear to be a consensus among stakeholders in relation to the policy they wish to see implemented in relation to the protection of minors, there seems little support for maintaining the status quo. Proposals include more self- and co-regulation, greater harmonisation and extending the AVMS Directive rules on protection to other online content.

Overall extension of the provisions of the AVMS Directive which protect minors would be a positive step, as it would help to fill the gaps in Irish legislation exposed by developments in the use of media platforms.

Question 2.3.

Section 28(5) of the 2009 Act states that the Compliance Committee of the BAI (a committee established under the 2009 Act) shall review on an ongoing basis the extent to which the television broadcasts of broadcasters under the jurisdiction of another Member State which are wholly directed towards audiences in the State comply with broadcasting codes. Moreover, Section 48(14)(b) of the 2009 Act states that where a matter has been the subject of multiple complaints made in respect of a broadcast transmitted from another jurisdiction targeted at audiences in the State, the Compliance Committee may review the matter concerned and report the findings arising out of such review to the Minister for Communications, Climate Action and Environment ("*Minister for Communications*") in such form and manner as the Committee thinks fit.[12] This appears to

[12] The legislation also refers to the Committee's ability to report to the "relevant public body". However, this term is not defined or used elsewhere in the legislation, and it is not clear to which bodies it may refer (i.e., within or outside the jurisdiction).

be intended as an observation/reporting role designed to identify specific concerns about potential avoidance rather than an effort to impose direct obligations in conflict with the country-of-origin principle.

In March 2017 the BAI launched its new General Communications Code ("**GCC**") setting out general rules and principles applicable to audio visual service providers in Ireland. As a code, it does not have the legally binding force of legislation although viewers and listeners have a right to complain to the BAI. The BAI will assess the complaint and may carry out enforcement actions such as issuing compliance notices or warning notices to the contractor or broadcaster. The GCC is explicit in stating that it will apply to all commercial communications carried on broadcasting under contact with the BAI or established under statute, but will not apply to commercial communications carried on broadcasting services licensed in other jurisdictions. This demonstrates respect and acceptance of the country-of-origin principle.

Section 3 of BAI's 2016 Access Rules emphasises the necessity of compliance with the provisions of the Access Rules for those broadcasters within the jurisdiction of Ireland but only in relation to levels of subtitling, sign language and audio descriptions that broadcasters licensed in Ireland will be required to provide. It states that the Rules shall not apply to other services commonly received in the State but licensed in the United Kingdom or in other jurisdictions. In addition, however, it states that the BAI reserves the right to extend the Rules and their applicability to new services licensed by the BAI under the Broadcasting Act 2009 from time to time, and that the BAI will make this assessment on a case-by-case basis.

There have been no reported disputes in respect of the application of the country-of-origin principle. Likewise, there are no reported instances of providers established outside the EU targeting Irish audiences.

Question 2.4.

Position in Ireland

Regulation of the broadcasting sector in Ireland falls within the remit of several bodies:

- The BAI issues broadcasting licences and deals with media concentration and aspects of pluralism in that context. Under Section 24 of the Broadcasting Act 2009, the BAI is independent in the performance of its functions.
- The Commission for Communications Regulation ("**ComReg**") is the statutory body responsible for the co-ordination, assignment and licensing of the associated radio frequencies to broadcasting services. ComReg's independence in the exercise of its functions is provided for in Section 11 of the Communications Regulation Act 2002.

- The Competition and Consumer Protection Commission ("CCPC") is the statutory body responsible for enforcing competition and consumer protection law in all sectors of the economy, including the media sector. It is responsible for the review of notifiable mergers, including media mergers. The CCPC is independent in the performance of its functions, under Section 9(5) of the Competition and Consumer Protection Act 2014.

Responsibility for the development of policy and the legislative framework for broadcasting in Ireland rests with the Department of Communications, Climate Action and Environment ("DCCAE"). The Minister for Communications also has a role in the review of media mergers from a media plurality perspective. That said, the Minister's regulatory remit is limited under statute: his review takes place after completion of the CCPC's competition-based review; is limited to the application of specified criteria in assessing whether the proposed transaction would be contrary to the public interest in protecting media plurality; requires, in cases of concern, the preparation of a report by the BAI; and is subject to judicial review by the High Court.

Digital and print media in Ireland are self-regulated by the Press Council of Ireland, which appoints the Press Ombudsman. The Press Council and Press Ombudsman are independent, in that they are free from State interference. The Press Council's independence is provided for by Schedule 2 to the Defamation Act 2009, under Section 44 of which (and, more particularly, the Defamation Act 2009 (Press Council) Order 2010 order made thereunder) it is recognised as a regulatory body for the press with responsibility for appointing the Press Ombudsman. The Press Council and the Press Ombudsman's responsibilities include considering complaints about newspapers, magazines and online-only news publications.

Analysis

It follows that there are no legal obstacles to independent regulation of the media in Ireland. Several bodies play a role in regulating the Irish media sector and their independence is guaranteed by statute. The role of the Minister for Communications, while not independent, is also clearly defined and circumscribed by statute. Furthermore, we are not aware of any problems of undue political or commercial pressure being placed on media regulators in Ireland. Against this tradition, an EU independence requirement is thus likely to be of little practical significance.

Nevertheless, regulatory conformity would certainly have advantages. Independent media regulation is of course desirable *per se*: enshrining these values would be a good thing for the EU more generally. Media operators may also benefit from the certainty afforded by a requirement that regulators would act independently in the public interest and to a similar/minimum set of standards.

Question 2.5.
The key areas of contention have been: (i) media concentration; (ii) funding of public service broadcasting; and (iii) rules on commercial communications.

Media Concentration
Media concentration is seen as a concern in Ireland. Media mergers in Ireland are governed by the Competition Act 2002 (as amended). A "media merger" is defined as a merger or acquisition involving two or more undertakings carrying on a "media business", which is defined as the business of:

(a) the publication of newspapers or periodicals consisting substantially of news and comment on current affairs, including the publication of such newspapers or periodicals on the internet;
(b) transmitting, re-transmitting or relaying a broadcasting service;
(c) providing any programme material consisting substantially of news and comment on current affairs to a broadcasting service; or
(d) making available on an electronic communications network any written, audio-visual or photographic material, consisting substantially of news and comment on current affairs, that is under the editorial control of the undertaking making available such material.

Media mergers have been subject to a special form of control since 2003. However, between 2003 and the introduction of the current system in 2014, the role of the Minister for Enterprise, Trade and Employment in protecting media plurality was ill-defined and never exercised. Following the report of an Advisory Group on Media Mergers in 2008, legislative proposals were made which finally saw light in the Competition and Consumer Protection Act 2014 (the "*2014 Act*"). The 2014 Act introduced a statutory definition of media plurality and sets out the relevant criteria to be applied by the Minister for Communications in assessing the merger.

Media mergers are now subject to an additional layer of assessment compared with non-media mergers. In addition to the role of the CCPC, which assesses media mergers on pure competition grounds, the Minister for Communications is responsible for considering media mergers from the perspective of plurality of the media. In particular, the Minister must determine *"whether the result of the media merger is likely to be contrary to the public interest in protecting plurality in the media business". "Plurality of the media"* is defined to include both diversity of ownership and diversity of content. In cases of concern, the Minister must request the BAI to produce a report on the merger.

For changes of control over entities operating radio and television stations, there is also a separate process requiring notification to the BAI. Under the Broad-

casting Act 2009, the BAI must consent to a change of control over the holder of a broadcasting contract or television programme service contract (licence). The BAI is required, in its review, to have regard to the desirability of allowing any person or group of persons to have control of or substantial interests in an 'undue number' of sound broadcasting services or an 'undue amount' of communications media in a specified area. This notification process is separate and additional to the notifications to the CCPC and the Minister described above.

Since the advent of the current media merger regime in 2014, 15 media mergers have been notified to the Minister for Communications. Most notably, the proposed acquisition in 2017 of CMNL Limited, a regional newspaper group, by Independent News and Media Holdings Limited, publisher of Ireland's best-selling national broadsheet, was withdrawn before the Minister could make a final decision. The BAI, in its report, had recommended that the Minister attach a number of conditions to any approval given to the transaction.

More generally, concerns have been expressed at a political level regarding plurality of media ownership in Ireland. The Media Ownership Bill 2017 was introduced in Dáil Éireann (the lower house of the Irish Parliament) in January 2017. That Bill, if enacted, would have further amended the Competition Act 2002 to enable the Minster for Communications to take retroactive measures regarding the media sector. Ultimately, the Bill, which was introduced by an opposition party, was defeated in parliamentary proceedings. However, given the high-profile nature of the concerns giving rise to the defeated draft legislation, there may be future legislative developments affecting the media sector.

Funding of public service broadcasting

In recent years, Ireland's public service broadcaster, RTÉ, has come under scrutiny by the European Commission. Newstalk, a rival radio station, submitted a complaint in 2014 regarding the Irish State's oversight of RTÉ's use of licence fee funds. According to Newstalk, RTÉ's use of licence fee funds was in breach of EU rules regarding State aid and RTÉ was using this money to subsidise commercial activities, providing it with an unfair advantage. Newstalk also complained that RTÉ was unfairly undercutting radio advertisement prices, by selling below cost. In August 2017, the European Commission closed its investigation, finding no evidence of illegal State aid. The Newstalk complaint is similar to a 2008 complaint made by TV3, a rival television station. Concerns were also raised in the early part of the decade by a group of national newspapers.

On a related note, there have recently been proposals to amend existing Irish arrangements around the payment of licence fees. Currently, holders of television sets are required to pay a licence fee which is collected by Ireland's postal operator, An Post. There is a reported 13.75% evasion rate, resulting in annual

losses of approximately €40 million. According to some media sources, it is proposed to invite other operators to tender for the provision of the licence fee collection service.

In addition, although the DCCAE had recommended that the television licence be extended to include other items such as computers, laptops and tablets, it is understood that no such proposals have been made at the time of writing.

Commercial Communications

The BAI General Commercial Communications Code ("GCCC") is necessitated by Section 42 of the Broadcasting Act 2009. The effect of the GCCC is reviewed at least every 4 years and a report is then published. The GCCC was updated in 2011, 2013 and 2017. The latest review began in 2014 with the aim of incorporating the views of all stakeholders by opening up a consultation period, the findings of which were published in the BAI *Report on the Effect of the BAI General Commercial Communications Code 2010*. The new GCCC came into effect in June 2017.

The new code is based on four key principles. Firstly, commercial communications must be legal, honest, decent and truthful. Secondly, commercial communications must respect human dignity and not cause offence or harm. Thirdly, communications must be transparent. The fourth principle acknowledges the special rules which are in place for the specific purpose of protecting children.

A key change made to the GCCC in 2017 was the clear distinction between product placement and sponsorship. The code now states that: if a product or service is built into the action of the programme, it is product placement; and if sponsor announcements or references are shown during a programme but are not part of the plot or narrative of the programme, they qualify as sponsorship.

Analysis

The first two issues noted above do not lend themselves to further harmonisation through the AVMS Directive. The regulation of commercial communications is addressed in the current Directive and the legislative proposal adopted in May 2016.

Question 2.6.

There is no specific local statutory provision which regulates targeted advertising in Ireland. Instead, it is expected that companies adhere to the general principles of the Advertising Code and Code of Ethical Business Practice of the Advertising Standards Authority of Ireland ("ASAI"). The ASAI's code states that all marketing should be "legal, decent, honest and truthful", prepared with "a sense of responsibility to consumers and to society" and in accordance with the "principles of fair competition generally accepted in business".

There is currently a legislative proposal before the Oireachtas (Irish Parliament) that could create new rules around the targeted advertisements of alcohol products in Ireland and there are also standards around the advertising of alcohol in Ireland that come from industry good-practice guides. This guidance recommends that no advertisement can appear in Irish print or broadcast without a pre-clearance check that will ensure the advertisement conforms to certain rules (e.g., does not feature anyone who appears to be under the age of 25 or associate alcohol with social success). When it comes to online advertising there is also specific guidance around what kind of sites (must have an adult audience profile of 75% or greater) and what areas of sites can be used (cannot exceed 25% of the total advertising space available on the site).

With regard to targeted advertisements using cookies to personalise content, there are a number of provisions concerning the storing and accessing of information on terminal equipment set out in Statutory Instrument No. 336 of 2011 which implemented the ePrivacy Directive into Irish law. This requires at a minimum that clear communication is used when asking a user to consent to cookies usage. The Office of the Data Protection Commissioner ("ODPC") has stated that it is particularly important that the requirements are met where third party or tracking cookies are being used in order to achieve targeted advertising. Accordingly the ODPC has issued minimum compliance guidance when using cookies to personalise content. When the General Data Protection Regulation ("*GDPR*") comes into effect in May 2018, the use of cookies to craft targeted advertisements will be subject to an overhaul due to the new rules around consent, data minimisation and enhanced privacy rights. Accordingly we would welcome further harmonisation of initiatives in light of the GDPR around the offering of targeted advertising across the EU.

An Internet Content Governance Advisory Group was established by the then Minister for Communications, Energy and Natural Resources to consider the existing national regulatory and legislative frameworks governing internet content. In May 2014, the Group produced a report where made several recommendations. These focused on increased oversight regarding child internet safety, especially targeting online abuse and cyberbullying.

Question 2.7.

The Copyright and Related Rights Act 2000 (the "*2000 Act*") gave effect to Council Directive No. 93/98/EEC on Harmonising the Term of Protection of Copyright. The term 'broadcast', as amended by Section 183(a) of the 2009 Act, is defined as "a transmission by wireless means, including by terrestrial or satellite means, whether digital or analogue, for direct public reception or for presentation to members of the public of sounds, images or data or any combination

of sounds, images or data, or the representations thereof, but does not include transmission by means of MMDS or digital terrestrial retransmission".

In relation to the ownership of copyright, Section 174 of the 2000 Act provides that the owner of copyright shall have the right to grant or refuse authorisation for cable retransmission of a broadcast or cable programme from another Member State of the EEA in which the work is included.

Section 103 of the 2000 Act relates to the reception and retransmission of broadcasts in cable services. It permits cable operators based in Ireland to retransmit works (including audio-visual works) protected by copyright that are broadcast in the State on the national cable programme service without obtaining permission from the copyright holders or paying retransmission fees. This has the effect that copyright in these works is not preserved when they are transmitted by a cable company based in Ireland.

Question 2.8.

Some of the main barriers to cross-border portability of digital content in Ireland include geoblocking and country-specific contracts for services. In the European Commission's report on "Identifying the main cross-border obstacles to the Digital Single Market and where they matter most", 40% of Irish consumers said they used online streaming services for accessing content and 51% considered the ability to access such content when abroad was an "important" factor when choosing a service provider.

While copyright licensing issues for streamed content could provide a justification for service providers limiting user access depending on the country they are in, and in turn address the data minimisation principles of Recital 28, Recital 39 and Article 6(1) of GDPR, considering the harmonisation principles of GDPR and the right to data portability, there could be grounds for reconciling cross-border access to digital content with the new data protection regime. Any obligation on the service provider to check or control the country of residence of the consumer risks being viewed as unduly onerous and may conflict with the data minimisation principles under the GDPR.

3. Digital infrastructures

Question 3.1.

Ireland had no rules on net neutrality in place before the adoption of Regulation (EU) 2015/2020 (the "*Net Neutrality Regulation*").

Article 5(1) of the Net Neutrality Regulation provides that national regulatory authorities ("*NRAs*") shall publish reports on an annual basis regarding their monitoring and findings, and provide those reports to the European Commission and to the Body of European Regulators for Electronic Communications

("*BEREC*"). ComReg is the NRA for the purposes of the Net Neutrality Regulation in Ireland. It published its first Implementation Report in relation to the Net Neutrality Regulation in May 2017.

Zero rating was introduced in Ireland as early as 2015, by the subsidiary of 3 Ireland, '48'. 48 offered a zero rated option whereby users were given unlimited usage of 'Whatsapp' outside 48's normal monthly data limits. In June 2016, Meteor became the first major mobile provider in Ireland to offer a zero-rating deal and allow customers to use Facebook, Twitter and Instagram without counting it towards their data allowance. In the same month, 3 Ireland announced that its phone customers would be given six months' "unlimited" music streaming through 'Deezer', a competitor of both Spotify and Apple Music. At the time of introduction, Maeve O'Malley, director of Meteor/Eir mobile, commented that, *"there is no net neutrality impact with zero rating. It is not currently expressly prohibited."*

In its Draft Electronic Communication Services Strategy 2017 – 2019, ComReg notes that *"while zero-rating may offer some benefits for consumers there have been concerns raised in relation to the practice on competition and net neutrality grounds"*. From a competition point of view, "the concern is that the practice of zero-rating may enable network operators to pick winners by tilting the playing field in favour of particular Over-The-Top ("*OTT*") service providers. A zero-rated OTT service provider would have an advantage over rivals whose end-users would have to pay data charges to use".

Question 3.2.

The DCCAE published the National Broadband Plan ("NBP") in August 2012. The NBP is a Government-wide initiative to deliver high-speed broadband services to all businesses and households in Ireland. Minister for Communications Denis Naughten, charged with the NBP, recently claimed that when he entered office last year, only 52% of premises in Ireland had access to high-speed broadband. It has since risen to 61%.

The NBP defines high speed broadband as a minimum speed of 30Mbps download, which would meet the European Commission's 'Digital Agenda for Europe' target of 100% coverage with 30 Mbps by 2020. This is being achieved through a combination of:

- commercial investment by the telecommunications sector;
- state intervention in those areas where commercial providers acting alone will not provide this essential service.

The State Intervention Strategy sets out the Government's approach to ensure that High Speed Broadband is made available to all households and businesses in

the country where there is no existing or planned commercial network. This non-commercial High Speed Broadband area is known as "The Intervention Area".

On 4 April 2017, the Minister for Communications announced that he had entered into an agreement with Eir in relation to a Commercial Deployment Commitment, in consequence of which Eir has committed to deploy a FTTH network passing approximately 300,000 premises (the "*300K network*") by the end of 2018. The Minister accordingly revised the proposed Intervention Area for the NBP. European Regional Development Funding is being used to help with the scheme.

Question 3.3.

ComReg is the statutory body responsible for the management of radio spectrum in Ireland. To assist ComReg's management of the radio spectrum, ComReg regularly sets out and updates its spectrum management strategy.

A key role of the DCCAE is the development of policies for the regulation and optimal use of Ireland's national radio frequency spectrum, underpinned by an appropriate legislative framework. Spectrum policy is part of the national policy governing the telecommunications sector in Ireland, which also covers next generation broadband, electronic communications services and international connectivity. The DCCAE also has the responsibility of developing national broadcasting policy and associated spectrum use.

The Communications Regulation Act 2002 as amended (the "*2002 Act*"), the Common Regulatory Framework (including the Framework and Authorisation Directives as transposed into Irish law by the corresponding Framework and Authorisation Regulations), and the Wireless Telegraphy Acts 1926 to 2009 set out, amongst other things, powers, functions, duties and objectives of ComReg that are relevant to the management of the radio frequency spectrum in Ireland.

In fulfilling its spectrum management function, ComReg carries out a range of activities including the:

- promotion of Ireland's interests in international fora;
- allocation and assignment of radio spectrum in Ireland;
- licensing of radio spectrum for a wide variety of uses;
- monitoring of radio spectrum usage in Ireland, including the enforcement of licence conditions and equipment standards; and
- promotion of Ireland as an ideal location for spectrum development using Test and Trial Ireland.

ComReg's primary objectives in carrying out its statutory functions in the context of electronic communications are to:

- promote competition;
- contribute to the development of the internal market;
- promote the interests of users within the Community;
- ensure the efficient management and use of the radio frequency spectrum in Ireland in accordance with a direction under Section 13 of the 2002 Act; and
- take the utmost account of the desirability of technological neutrality.

Question 3.4.
ComReg is the NRA for the purposes of Regulation (EU) 2015/2120 in Ireland. Section 11 of the 2002 Act provides that the *"Commission shall be independent in the exercise of its functions"*.

4. Data in the digital economy

Question 4.1.
In May 2017, the Department of Justice and Equality published the General Scheme of Data Protection Bill 2017 (the "*Bill*"). The General Scheme outlines the proposed structure and content of the Bill, a draft of which is due to be published in the Autumn of 2017.

The Bill will be designed to give effect to, and provide for derogations from, the GDPR. Further, the Bill will transpose into national law the Law Enforcement Data Protection Directive (EU) 2016/690 which concerns the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offence, and the free flow of such data.

The General Scheme envisages that current data protection authority in Ireland, which is the Data Protection Commissioner, will be replaced by a new legal entity to be named the Data Protection Commission ("*DPC*"), with the potential for up to three individual Commissioners to be appointed. This is stated to be partly to provide for additional capacity for dealing with the expected additional workload under the GDPR, and the "*one stop shop*" in particular. One Commissioner will be appointed as Chairperson.

The General Scheme also envisages the enactment of secondary legislation under the Bill, once it is enacted and commenced, and that the Bill will provide for a number of regulation-making powers, in connection with the GDPR. For example, Article 23 of the GDPR permits, by means of a legislative measure, restrictions on the exercise of data subject rights which are necessary and proportionate in a democratic society in order to safeguard important objectives of general public interest. The General Scheme envisages that the Bill will grant broad ministerial powers, following consultation with the DPC, to restrict organisations' obligations and individuals' rights via regulations, in so far as necessary

to *"safeguard important objectives of general public interest"*. The restrictions will be required to respect the essence of the right to the protection of personal data and be a necessary and proportionate measure. A non-exhaustive list of *"important objectives of general public interest"* will be set out in the Bill, such as to safeguard national security, defence and international relations or to prevent threats to public security and safety.

The Bill is still at a preliminary stage and is likely to change considerably before it is enacted.

Question 4.2.

In order to be ready to comply with the GDPR by 25 May 2018, Irish businesses are examining their existing data processing and the legal basis on which they carry out such processing now and intend to do so under the GDPR regime, reviewing their data protection policies, procedures and controls and identifying any gaps that need to be addressed. Companies need to consider the life cycle of data, from collection to deletion, when considering whether their data processing is necessary, relevant and proportionate and when updating their data protection policies and practices. Those for whom the appointment of a Data Protection Officer may be mandatory are also determining the parameters of the role and how it will be filled and interact with existing organisational structures. Many will also need to engage in internal training to ensure that staff are made aware of the requirements of the GDPR and its impact on their roles in connection with the processing of personal data.

Many business have commenced their GDPR preparations, however a significant proportion have yet to begin. Since GDPR preparations can be large and complex projects, potentially requiring substantial changes to be made, business who have not begun their preparations should consider doing so now.

Question 4.3.

The Irish Government has identified the Internet of Things as an area of opportunity for Ireland to capitalise on its strong international reputation as an ideal jurisdiction in which to locate and further develop cutting edge businesses and technologies. Ireland is home to numerous IoT research and development centres and hubs. Dublin is emerging as a leading location for Smart City and IoT innovations with National Geographic recently citing Dublin as *"leapfrogging the competition in the race to be a smart city"*.

While there are several IoT projects and developments currently taking place in Ireland, there has been limited discussion in terms of regulation and policy. In ComReg's ECS Strategic Statement 2017 – 2019, it is noted that it is *"uncertain at present whether this wave of innovation will create any additional requirements in*

terms of regulation". It further predicts that for Ireland, by 2020 the number of connected devices will exceed 1 million and "while the nature and functions of these new connected devices is as yet unknown, key areas currently benefiting from IoT services include automotive, ehealth services, smart metering/smart grids, smart homes, smart cities, industry/automation and agriculture".

The Strategic Statement also notes that the advent of IoT will yield particular challenges for ComReg. In particular, the connectivity requirements for IoT devices are particularly wide and will require new service offerings to meet the individual requirements. In addition, the rollout of IoT devices may require significant numbering resources. Given the significant potential for life-style and productivity enhancement associated with IoT, ComReg is also *"conscious of its role in relation to the facilitation of innovation and investment."*

Question 4.4.

The right to the erasure of personal data is set out in Section 6 of the Data Protection Acts 1988 and 2003.

The first 'right to be forgotten' case brought in the Irish courts following the 'Google Spain' case came before Dublin Circuit Civil Court in May 2016. Mark Savage, a former local election candidate, challenged a decision of the Data Protection Commissioner ("DPC") which supported Google's refusal to remove a link to the website 'Reddit.com' referring to him as *"North County Dublin's homophobic candidate".*

The web page appeared in Google's search results when a search was carried out against Mr Savage's name. Mr Savage had run as a candidate for public office as Councillor in the 2014 local elections, with election literature referring to "*Gay Perverts cavorting in flagrante on the beach in broad daylight*". Mr Savage argued that the Reddit page presented inaccurate information as it presented him as a homophobe without any qualification. He asked Google to delist the Reddit search result.

Google refused to take down this link. It maintained that, as a public figure, Mr Savage had joined a debate on matters relating to the gay community. Google added that, as this information related to Mr Savage's public persona, it was in the public interest that internet users have access to his political and cultural views.

The DPC took the view that the inclusion by Google of the link could not be considered prejudicial to Mr Savage's fundamental rights and freedoms. In particular, the DPC took the following criteria into consideration:

- Is the data subject a public figure?
- Is the data accurate?
- Is the data relevant and not excessive?

- Is it clear that the data reflects an individual's personal opinion, or does it appear to be verified fact?
- In what context was the information published? Was the content voluntarily made public by the data subject?

The DPC indicated that the text of the URL expressed the opinion of the poster and was not expressed as being factually accurate. The DPC added that the public interest and freedom of expression outweighed the right to privacy in this case.

Mr Savage appealed the DPC's decision to the Circuit Court. He argued that users of the internet are increasingly reliant on it for ascertaining information and the need for accuracy regarding factual information is of *"paramount importance"*. He added that a user would form the view that he had run in the local elections as a homophobic candidate, due to how the URL title was displayed by Google. He argued that the URL title had the appearance of a verified fact, without any qualification, which was inaccurate, excessive and inadequate.

The court found that the decision of the DPC "fell into error" on the basis that it was "far from clear" that the URL title was the expression of the poster's opinion. While accepting that the procedures followed by the DPC were appropriate, the court disagreed with the findings arrived at and took the view that Mr Savage's fundamental rights and interests had been prejudiced. The court decided that the balance of rights fell in favour of Mr Savage, despite that he was a public figure, and overturned the DPC's decision.

An appeal by the DPC and Google Ireland against the finding of the Circuit Court was heard by Mr Justice White in the High Court in May this year. The High Court has reserved judgment so the judgment is not yet available.

ITALY

Prof. Oreste Pollicino* • Avv. Mario Siragusa**
Avv. Fausto Caronna*** • Prof. Roberto Mastroianni****

1. Internal Market and electronic commerce: Internet and e-commerce

Question 1.1.1

Since the implementation of the E-Commerce Directive through the Legislative Decree no. 70 dated April 9th 2003, Italian Courts have addressed several interpretative issues related to the definition of Internet Service Providers (ISPs) and, in particular, to the scope of application of the liability exemptions provided for by Article 14 et seq. of the Directive.

In this respect, national Courts have identified a distinction between *active* and *passive* hosting providers. This distinction has no grounds in the text of the e-Commerce Directive (nor in that of the Legislative Decree no. 70/2003), but has been drawn on the assumption that the said liability exemptions should only apply to hosting providers of merely *technical*, *automatic* and *passive* nature pursuant to Recital 42 of the E-Commerce Directive. These developments have led Italian Courts to apply stricter standard of liability when the functioning of digital platforms reveals a significant degree of interaction between the hosting provider and the activity or information stored on request of the recipient of the service. On the basis of specific features (including, but not limited to, the inser-

* Full Professor of Constitutional Law at Bocconi University Milano and Of Counsel, Portolano Cavallo Studio Legale; Chapter 1.1, 1.4 and Chapter 3.
** Partner of Cleary Gottlieb Steen & Hamilton LLP.
*** Full Professor of EU law at Università "Federico II°" Napoli; Chapter 2.
**** Senior Attorney of Cleary Gottlieb Steen & Hamilton LLP Chapter 1.2, 1.3 and Chapter 4.

tion of clauses within the terms and conditions of the service; the organization and selection of the information provided by customers, including by providing search tools enabling users to search for content by keyword or by indexing and selecting videos), it is then assumed that hosting provider shave a degree of control over third parties content and are then excluded from the liability exemptions set forth by the E-Commerce Directive.

Recently, some judgments have specifically tackled this problem. In particular, it is worth mentioning the recent decision of the Court of Torino dated April 7th 2017,following a lawsuit for online copyright infringement. The Court rejected the plaintiff's argument that liability exemptions were not applicable to YouTube because of its active role in selecting and organizing online content.

A few weeks later, the Court of Appeal of Rome has dealt with a similar case where an action against a video-sharing platform was at hand. In its judgment, the Court of Appeal of Rome found that the concerned online platform actually played an active role through the arrangement of the content published by the recipients of its services and ruled, accordingly, that no liability exemption was applicable.

The interpretative issue is self-evident, but it is the consequence, among others, of the nature of judicial decisions which are based on a case by case approach and, in civil law systems, are not legally bound by previous judicial decisions.

In addition to the above, another interpretative issue derives from the implementation of Article 14 of the E-Commerce Directive in the Italian legal order. Most notably, unlike the E-Commerce Directive, Article 16 of the Legislative Decree no. 70/2003 expressly grants to the competent court or administrative authority the power to order the removal or disabling of the access to illegal content. Said order is considered a requirement for the hosting provider to take the necessary steps to remove or disable the access to information. Amongst Italian courts, then, it is debated whether ISPs should be kept in any cases immune from liability in the absence of such an order or whether the same may be deemed liable also on the ground of different circumstances.

Question 1.1.2.

The test for liability developed by the Court of Justice of the European Union in the *L'Oréal v. eBay* case leaves national courts room for evaluating the specific circumstances of the cases at hand and whether they may affect the application of the liability exemptions to hosting providers.

As it is well known, the test is based on two steps.

The first one requires assessing whether the online platform at stake acts as a mere intermediary, without playing an active role. Here, the difficulty lies in

the interpretation of the role of ISP, depending essentially on the judicial interpretation of the definition provided for by the e-Commerce Directive as implemented in the national legal systems. The role of hosting providers, in fact, has significantly changed over these years and, accordingly, courts' interpretation has become more and more influential to determine whether digital platforms fall within the scope of the E-Commerce Directive.

The second step requires assessing the degree of awareness of online platforms. In other words, online platforms which are aware of the illicit character of online content published by the recipients of their services cannot benefit from the liability exemptions provided for by the E-Commerce Directive. This approach, also known as *notice and take down*, grants to right holders the power to obtain the removal or the block of access to illegal content. But, even in this respect, there are some interpretative issues, concerning in particular the subject which can notice to an online platform the existence of illicit content or the form of the notice (for example, if for such not to be given a mere cease and desist letter suffices or an order of the competent national authority is necessary).

Looking at how Italian courts have dealt with this test in the aftermath of the *L'Oréal v. eBay* case, it comes out that the inherent ambiguity of the same made possible for the relevant parties to argue in both senses on the grounds of the ruling of the Court of Justice. Also, as noted in the answer to Q1.1.1, Italian courts have speculated on the distinction between *active* and *passive* hosting providers by relying on some features allegedly revealing a degree of control over content. However, in the absence of specific criteria and any legal grounds for applying a stricter standard of liability, this trend may negatively impact legal certainty.

Question 1.1.3.

The notice and take down regime does constitute an appropriate solution to handle claims of intellectual property rights infringements, as a prompt removal on request of the right holders is crucial to prevent significant damages occurring as a consequence of unauthorized use of protected works. The same solution can probably turn out to be appropriate also when it comes to claims related to the unauthorized disclosure of personal data. Generally speaking, this approach is likely to increase the workload of online platforms, thus impacting their capacity to grow up and develop new services due to the resources necessary to manage all the requests.

In addition to the above, the notice and take down regime may be effectively implemented with regard to hate speech and defamatory content, even though some critical point have to be considered in this respect. Claims to remove content that constitutes hate speech or defamation, except for manifestly illicit conducts, requires ISP to investigate the degree of permissible exercise of freedom

of speech, that is subject to different standard of constitutional protection in the US and Europe. This scenario may result in attributing to ISP a quasi-constitutional role while handling complaints for the removal of content in the absence of a judgment of a court declaring the same to be illicit. This way, taking an extreme view, ISP would be required to exert a kind of collateral private censorship that, most likely, would support the existence of an editorial responsibility. A similar problem is likely to come up with respect to claims of copyright infringements, as the *prima facie* unauthorized use of copyrighted materials may be justified as *fair dealing*.

In this regard, it is worth observing that the Italian Communication Authority (AGCOM), through resolution no. 680/13/CONS, adopted a regulation on online copyright enforcement with a view to reducing the enduring and massive violations of copyright via electronic communication systems. Said regulation does formally embody a notice and take down approach, by which right holders and their representatives are entitled to file complaints before AGCOM according to a special accelerated procedure to obtain the removal of the concerned content or the block of access to the same.

Question 1.1.4.

There are no specific cases to report showing difficulties with respect to the principles laid down by the *Scarlet v SABAM* (C-70/10) and *SABAM v Netlog NV* (C-360/10) cases. As far as the prohibition of a general obligation to monitor is concerned, Article 17 of the Legislative Decree no. 70/2003 reflects the principle stipulated by Article 15 of the E-Commerce Directive. The only judgments challenging, to a certain degree, this principle required hosting providers to implement specific systems or software aimed at preventing users from uploading *ex novo* the same content previously subject to take down measures.

Recently, on May 8th 2017, the Court of Milan specifically mentioned the *Scarlet* case in order to justify the injunction against an online platform ordering to take the necessary steps to avoid the repetition of the copyright infringements at hand. The Court of Turin, likewise, in the judgment released on April 7th, 2017, ruled that YouTube shall continue to use the Content ID software. At present, there is no specific speculation on whether such requirement may call into question the prohibition to implement general monitoring measures.

Furthermore, the *Scarlet v SABAM* and *SABAM v Netlog NV* cases also called for the need to strike a fair balance between copyright protection, on the one hand, and the protection of freedom of speech, personal data and freedom to conduct business, on the other one. Ordinary courts refer to these criteria (among others, see Court of Rome, judgment of July 15th, 2016) most notably to support the adoption of measures for copyright enforcement as a proportionate remedy,

whose interference with the protection of other fundamental rights is not overbroad and excessive.

Question 1.2.1.

Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees[1] (the "*CSG Directive*") was implemented in Italy by Articles 128 to 135 of Legislative Decree No. 206 of September 6, 2005 (the "*Italian Consumer Code*").[2]

Although the CSG Directive is a minimum harmonization directive, the Italian legislator chose to merely maintain the level of consumer protection provided for at EU level. However, as described below, Italian decisional practice and case law on the rules on legal guarantees has been deeply influenced by the aim to provide consumers with a high level of protection, which has resulted in some cases in a higher level of protection than that set out by both the EU and Italian legislator.

Within the last decade the Italian Competition Authority (the "*ICA*") focused on the enforcement of the rules on legal guarantees, carrying out about 40 infringement proceedings against sellers (and less frequently, producers) for unfair commercial practices resulting from breaches of the rules on legal guarantees.[3] In November 2010 the ICA also published informal *Guidance on the legal-guarantees regime*,[4] summarizing its reading of the content of the rules on legal guarantees and the resulting rights and duties for consumers and traders.

[1] OJ L 171/12.

[2] The CSG Directive was originally implemented by Legislative Decree No. 24 of February 2, 2002, which introduced Articles 1591 *bis* to *nonies* in the Italian Civil Code. Successively, these provisions have been incorporated in the Italian Consumer Code.

[3] The ICA is entrusted with the public enforcement of the rules on unfair commercial practices set forth by Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (the "UCP Directive"). Since 2014 the ICA is also entrusted with the public enforcement of the rules implementing Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (the "CR Directive"). Among the proceedings concerning the violation of consumer rights carried out by the ICA, see: decisions of December 12, 2015, No. 25759, case PS10042, *H3G-Sweep garanzia legale/commerciale;* November 4, 2015, No. 25702, case PS10035, *PC Italia-Sweep garanzia legale/commerciale* and March, 9, 2016, No. 25911, case PS9353, *Amazon Market Place-garanzia legale*.

[4] Available at http://www.agcm.it/consumatore/decalogo/5102-garanzia-del-venditore-guida-per-il-consumatore.html

In its decisional practice, the ICA focused its attention on the duty to inform consumers of the existence of the legal guarantee concerned and its content. Many of the infringements found by the ICA indeed concerned: (i) the lack of clear, adequate and comprehensive information provided to consumers on the content of the legal guarantee;[5] and (ii)the provision of information on the contractual guarantee likely to mislead consumers on the rights deriving from the legal guarantee.[6]

Furthermore, in several cases[7] the ICA found that sellers had refused to directly manage consumers' requests for assistance under the legal guarantees regime. The ICA found that they had merely diverted consumers' requests for assistance to the producers, thus making it difficult in practice for consumers to exercise the rights in the CSG Directive.[8]

Interestingly, in its most recent decisions,[9]the ICA accepted commitments from producers of large household appliances whereby they are, among other things, required to respond directly to consumers' requests for assistance, thus in fact shifting the legal guarantee obligation from the sellers to the producers.[10]In contrast, in *Amazon-Marketplace*,[11] the ICA merely required Amazon, when acting as an online platform (*Amazon marketplace*) and not as a seller, to provide clear

[5] See, among others, case PS9353, *Amazon-Marketplace-Garanzia legale*quoted above; decision of March 2, 2016, No. 25901, case PS9970, *Privalia-Sweep garanzia legale/commerciale*; July 25, 2012, No. 23768, case PS8030, *ESSELUNGA – Prodotti in garanzia.* See also decisions of September 7, 2011, Nos. 22755, case PS6378, *Telecom-Garanzia prodotti;* 22749, case PS3005; *H3G e One Italia–Garanzia prodotti*;22756, case PS6920, *Wind–Garanzia prodotti;* 22757, case PS6944, *Vodafone–Garanzia prodotti*; 22399, case PS3528, *Carrefour-Prodotti in garanzia*.

[6] See, among others, decisions of March 9, 2016, No. 25912, case PS10125, *Otis – Garanzia e responsabilità per ritardo*; December 22, 2015, No. 25805, case PS10039, *Philips-Sweep garanzia legale/commerciale*; April 16, 2014, No. 24887, case PS9230, *LIDL – Prodotti in garanzia*; December 20, 2013, No. 24715, case PS8714, *Sony- Garanzia legale.*

[7] See, among others, cases PS6378, *Telecom-Garanzia prodotti;* PS3005, *H3G e One Italia–Garanzia prodotti,* PS6920, *Wind–Garanzia prodotti;* PS6944, *Vodafone–Garanzia prodotti* and PS3528, *Carrefour-Prodotti in garanzia*quotedaboveand decisionsissued on 5 August 2010, No. 21457, PS2650, *UNIEURO – Prodotti in garanzia*, No. 21456, PS2416 – *MEDIAWORLD – Prodotti in garanzia* and No. 21454, PS2180, *EURONICS – Prodotti in garanzia*.

[8] See, among others, cases PS6378, *Telecom-Garanzia prodotti;* PS3005, *H3G e One Italia–Garanzia prodotti,* PS6920, *Wind–Garanzia prodotti;* PS6944, *Vodafone–Garanzia prodotti* and PS3528, *Carrefour-Prodotti in garanzia* quoted above and decisions issued on 5 August 2010, No. 21457, PS2650, *UNIEURO – Prodotti in garanzia*, No. 21456, PS2416 – *MEDIAWORLD – Prodotti in garanzia* and No. 21454, PS2180, *EURONICS – Prodotti in garanzia*.

[9] [TO BE COMPLETED (FINAL DECISIONS ARE EXPECTED IN OCTOBER 2017)]

[10] As it is well known, pursuant to the CSG Directive only the sellers are liable to the consumers for any lack of conformity of goods (see Article 3), though pursuant to Article 4 of the CSG Directive they are recognized a right of redress vis-à-vis any other previous intermediary and producer in the contractual chain.

[11] See case PS9353, *Amazon–Market place–garanzia legale* quoted above.

information about the actual seller of the goods in order to make it clear to consumers who the subject liable for the lack of conformity of the goods is. Thus, in this case the ICA appears to have considered that, as long as this information is adequately provided to consumers, compliance with the rules on unfair commercial practices and legal guarantees is ensured.

Finally, a controversial ruling in the Italian case law concerns Article 5(3) of the CSG Directive, pursuant to which "*[u]nless proved otherwise, any lack of conformity which becomes apparent within six months of delivery of the goods shall be presumed to have existed at the time of delivery*". Article 5(3) of the CSG Directive has been literally transposed into Article 132(3) of the Italian Consumer Code.

By limiting the presumption to the six months' period from the good's delivery, the above rule is arguably imposing on the consumer the burden of proof for any lack of conformity that becomes apparent afterwards. Nonetheless, in *Apple*[12]the Italian Council of State, Italy's Supreme Administrative Court – irrevocably upholding the ICA's decision of December 21, 2011, No. 23155, case PS7256, *Comet – Apple – Prodotti in garanzia* –in effectrepealed this provision. In particular, the Council of State took the view that, based on [the principle that consumers do not have to bear any costs when exercising their rights pursuant to the legal guarantees regime and in light of the purpose and *ratio* of the legal guarantees regime, consumers are only required to inform the seller of the lack of conformity within two months of the date on which they detect such lack of conformity. If consumers timely inform producers of the lack of conformity, then, as long as the defect concerned became apparent within 24 months from the delivery of the good, it is always on the producer to carry out an accurate assessment of the good's defect in order to ascertain whether a lack of conformity exists. No charges for such assessment may be imposed on consumers.

In other words, based on the Council of State ruling in *Apple*, as long as a defect becomes apparent within the 24 months' period covered by the legal guarantees regime, and it is timely reported by the consumer, it is always on the sellers or producers to demonstrate that no lack of conformity existed at the time of delivery.

Question 1.2.2.

According to the Digital Economy and Society Index (the "*DESI Index*"), the EU has progressed and improved its digital performance by 3 percentage points compared to 2016, but "*progress could be faster and the picture varies across Member States*".[13]Regarding Italy, Internet users engage in online activities much less than the average EU user: Italy ranks 25th out of 28 in the DESI Index 2017.

[12] Consiglio di Stato judgement of November 17, 2015, No. 5250.

[13] European Commission – Press release How digital is your country? Europe improves but still needs to close digital gap Brussels, 3 March 2017

In the European Commission's view, differences in national mandatory consumer contract law rules and a lack of clear contract law rules are among the key obstacles that hinder the development of the supply of digital content.[14]

Thus, the proposed CSDC Directive aims to fill the legal void in the *acquis communautaire* by fully harmonizing a set of key rules that are not yet regulated at the EU level. In particular, the proposed CSDC Directive: introduces rules on conformity of digital content and related remedies in cases of lack of conformity with the contract; provides for a right to terminate long term contracts; and regulates certain aspects concerning the modification of digital content to be supplied over a period of time.

Indeed, the above aspects are not currently regulated at the EU level: the CSG Directive does not apply to contracts for the supply of digital content, since it only applies to contracts for the sale of consumer goods(pursuant to Article 1(2)(b) "*consumer goods*" means "*any tangible movable item*"). Therefore, those who buy digital content cannot benefit from the various remedies provided under EU Law when there is a lack of conformity. At the same time, Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (the "*Consumer Rights Directive*") provides only a few fully harmonized rules for the supply of digital content, essentially concerning pre-contractual information requirements and the right of withdrawal.

While the proposed CSDC Directive represents a step forward in the right direction insofar as it will provide for an autonomous legislative instrument filling in the above gaps, it is arguably also open to criticism.

First, following the enactment of the proposed CSDC Directive, the EU regulatory framework will include unjustified diverging rules for digital content and other goods respectively. Contrary to the stated objectives of the legislative reform, this scenario might heighten consumers' uncertainty of their contractual rights, thus ultimately hindering the development of a genuine single market.[15]

[14] See Explanatory Memorandum to the Proposal for Directive on certain aspects concerning contracts for the supply of digital content (the "proposed CSDC Directive"); see also Recitals 3-4 of the proposed CSDC Directive.

[15] In its Report on the REFIT Fitness Check covering the six core horizontal EU consumer and marketing law directive, including the CSG Directive, the Commission reiterates that, in its view, coherence in the field of contract law is fundamental and confirms the need to maintain coherent rules applicable to both the online and offline sectors. Moreover, the Commission also makes clear that it is already actively assisting Parliament and the Council in their discussion on possibly expanding the scope of the proposed CSDC Directive to cover all sales channels.

In this regard, we refer in particular to Article 9 of the proposed CSDC Directive, pursuant to which "*[t]he burden of proof with respect to the conformity with the contract at the time indicated in Article 10 [i.e. at the time the digital content is supplied and/or occurring during the time over which the digital content is to be supplied pursuant to the contract] shall be on the supplier*". As made clear in the Explanatory Memorandum to the proposed CSDC Directive, this reversal of the burden of proof is not limited in time. The Commission argues that this is justified because digital content is not subject to wear and tear.[16]

The above rule radically differs from the rule on the burden of proof applicable to contracts for the sale of any tangible movable item, provided for in the CSG Directive.

While Article 9 of the proposed CSDC Directive arguably supports the rather "creative" reading of the CSG Directive's regime on the burden of proof asserted by Italian case law (see point 1.2.1 above), coherent and clear rules, applicable throughout the EU to both digital content and other tangible movable items, would arguably be preferable. Accordingly, further legislative action at the EU level is arguably needed.

Secondly, the proposed CSDC Directive makes reference to some rather vague and open concepts, which would leave a wide measure of discretion to national judges, creating possible discrepancies among Member States, as well as legal uncertainty. This arguably contradicts the maximum harmonization approach of the proposed CSDC Directive,[17] ultimately jeopardizing the single market objective of the reform.

For example, pursuant to Article 12(2) of the proposed CSDC Directive, in the case of a lack of conformity with the contract, "*the supplier shall bring the digital content in conformity with the contract pursuant to paragraph 1 within a reasonable time from the time the supplier has been informed by the consumer about the lack of conformity with the contract and without any significant inconvenience to the consumer, taking account of the nature of digital content and the purpose for which the consumer required this digital content*". Whilst "*reasonable time*" and "*significant inconvenience*" are flexible concepts that can be fleshed out on a case-by-case basis, they also leave a wide measure of discretion to national judges, leaving room for divergent interpretations, running contrary to the stated objectives of the proposed CSDC Directive.

A further example relates to the very scope of application of the proposed CSDC Directive. Pursuant to its Article 3(5), the proposed CSDC Directive shall not apply to "*services performed with a predominant element of human intervention by the supplier where the digital format is used mainly as a carrier*". It is not clear which

[16] See Explanatory Memorandum, page 12.

[17] See Article 4 of the proposed CSDC.

services would fall within this category, and thus outside the scope of the fully harmonized rules on contracts for the supply of digital content.[18]

Question 1.2.3.

While the rules on pre-contractual information requirements, the right of withdrawal and delivery conditions applicable to online and distance sale contracts have already been fully harmonized through the Consumer Rights Directive, the rules on legal guarantees applicable in the EU are still rather fragmented, including in relation to conformity criteria and how legal guarantees are enforced.

Indeed, the CSG Directive – which applies to the sale of tangible goods through any sale channels, including online and distance sales channels – is a minimum harmonization directive, which allows(and, as a matter of fact, has resulted in) significant differences among national provisions transposing the CSG Directive**.** Such differences in turn represent, according to the Commission, "*one of the main obstacles to cross-border sales*",[19] as they tend to: (i) generate additional costs for sellers, who must adapt to different contract rules in force in the various Member States where they export; and (ii)generate legal uncertainty about key contractual rights, undermining consumer confidence in cross-border purchases.[20]

The proposed Directive on certain aspects concerning contracts for the online and other distance sales of goods (the "*proposed Online Sales Directive*") aims to remove such obstacles through full harmonization[21] of the rules on conformity of goods, remedies in case of non-conformity and the modalities for the exercise of these remedies applicable to distance sales contracts[22] concluded between a seller and a consumer. At the same time, the CSG Directive would be amended to make sure that it only applies to "*contracts for the sale of consumer goods and associated guarantees, which are not distance sales contracts…*".[23]

[18] Jürgen Basedow points out for example that it is doubtful whether "*a telecom hotline supporting the operation of a real property platform be included or excluded from the scope of the directive*" (Basedow J., *European Contract Law and the Digital Agenda*, in Contratto e Impresa /Europa,(2) 2016, 423-437).

[19] See the Explanatory Memorandum to the proposal for a Directive on certain aspects concerning contracts for the online and other distance sales of goods, p. 2.

[20] See the proposal for a Directive on certain aspects concerning contracts for the online and other distance sales of goods, recitals 5-7.

[21] See Article 3 of the proposed Online Sales Directives.

[22] Pursuant to Article 2(e) of the proposed Online Sales Directives, "distance sales contract" means "*any sales contract concluded under an organised distance scheme without the simultaneous physical presence of the seller and the consumer, with the exclusive use of one or more means of distance communication, including via internet, up to and including the time at which the contract is concluded*".

[23] See Article 19 of the proposed Online Sales Directives, amending Article 1 of the CSG Directive.

While the Proposed Online Sales Directive takes the rules of the CSG Directive as a basis, in some cases it goes further than them, providing for a level of consumer protection higher than that in the CSG Directive.

For example, differently from the CSG Directive, pursuant to the proposed Online Sales Directive consumers would not have a duty to notify a defect in the goods to the seller within a certain period of time from its discovery. More importantly, the period for the shift of the burden of proof provided for by the proposed Online Sales Directive is extended from six months to two years.[24]

With regard to the above key aspects, the EU legal framework would thus have rules on distance sales that are significantly different from the rules on face-to-face sales.

As admitted by the Commission itself, this scenario would be unfortunate, also taking into account "*the increasing importance of the omni-channel distribution model (i.e. selling at the same time via multiple channels such as directly in a shop, online or otherwise at a distance)*". Therefore, the Commission anticipates that efforts should be made to ensure that "*consumers and traders will… be able to rely on a coherent legal framework, which is simple to apply everywhere in the EU*".[25]

Finally, our remarks concerning the use of vague concepts (such as "*reasonable time*" and "*significant inconvenience*") in the proposed CSDC Directive (see answer to Q.1.2.2 above) also apply in this context, as the same concepts are also present in the Proposed Online Sales Directive.

Question 1.2.4.
Please see answers to Q1.2.2 and Q1.2.3.

Question 1.2.5.
In our view, from a substantive point of view the current EU framework is effective overall in protecting consumers, even with respect to transactions with online platforms. This is also accomplished thanks to its technology-neutral principle-based approach.

Conversely, we believe that the main issues currently relate to guaranteeing effective enforcement of the Unfair Commercial Practices Directive 2005/29/EC (the "*UCPD*"), the Unfair Contract Terms Directive 1993/13/EC (the "*UCTD*") and the Consumer Rights Directive (together with the UCPD and the UCTD, the "*Directives*"), including and in particular with regard to cross-border enforcement.

[24] See Article 14 of the proposed Online Sales Directive. As noted in Q.1.2.2 above, the rule on the burden of proof provided for in the proposed Online Sales Directive is in line with the current interpretation in the Italian case law of the rules implementing the CSG Directive in Italy. However, our remarks above also apply here.

[25] See the Explanatory Memorandum to the proposed Online Sales Directive, page 3.

The proposal put forward by the European Commission for the reform of Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the "*CPC Regulation*")[26] in May 2016 (the "*Proposed CPC Reform*")[27] marks a step in the right direction. However, for the reasons illustrated below, we believe that there is scope to revise the Proposed CPC Reform with a view to further strengthening it.

The current framework in the CPC Regulation to coordinate national authorities in cases of consumer law infringements concerning several EU Member States (i.e., "widespread infringements") is widely considered to be insufficient and too loose, leading to unnecessary duplication of enforcement efforts, as well as possible inconsistencies in the application of EU consumer law (particularly with respect to the digital environment). This is so insofar as it is mainly based on a system of alerts and bilateral mutual assistance, while it does not foresee the possibility of joint actions by the national authorities.[28]

With a view to remedying these shortcomings, the Proposed CPC Reform envisages, among other things, that – whenever there is a reasonable suspicion of a "*widespread infringement with a Union dimension*" (i.e., harming consumers in at least three quarters of the Member States, accounting together for at least three quarters of the EU population), there should be one common procedure coordinated by the European Commission. Below these thresholds, for infringements involving at least two or three Member States (so called "*widespread infringements*" without a Union dimension),[29] the coordination would have to take place among the national authorities concerned, which may invite the European Commission to take up the coordination role.

[26] Regulation (EC) No. 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 364/1.

[27] Proposal for a Regulation of the European Parliament and of the Council on Cooperation between national authorities responsible for the enforcement of consumer protection laws, COM(2016) 283 final.

[28] However, it must be noted that – albeit in the silence of the law – national authorities have taken steps to strengthen their cooperation, through so-called "sweeps" (i.e., coordinated screenings of online e-commerce websites, carried out since 2007 in various sectors) and joint coordinated actions (i.e., coordinated positions in areas of common interest requiring traders concerned by widespread problematic practices to change them across the EU, since 2014).

[29] Pursuant to Article 3 of the Proposed CPC Reform, a "widespread infringement" means: "*(1) any act or omission contrary to the laws that protect consumers' interests that harmed, harms, or is likely to harm the collective interests of consumers residing in at least two Member States other than the Member State where the act or omission originated or took place, or where the trader responsible for the act or omission is established, or where evidence or assets pertaining to the act or omission are to be found; irrespective of whether the act or omission is ongoing or has ceased; or (2) any acts or omissions contrary to the laws that protect consumers interests that have common features, such as the same unlawful practice, the same interest being infringed or that are occurring concurrently, in at least two Member States*".

In our view, the Proposed CPC Reform still appears to be insufficient to effectively tackle the issue of cross-border enforcement, in light of the significantly high level of the thresholds for the common actions coordinated by the European Commission.

Accordingly, we believe that it would be preferable to have a single, lower threshold (corresponding to three Member States) to trigger the European Commission's coordination action.

The advocated different single threshold would be coherent with the framework in place for cooperation among national competition authorities within the European Competition Network,[30]and clearly it would boost cross-border enforcement under the European Commission's lead. Moreover, a lower single threshold would also strengthen national enforcement, which – being brought under the central role of the European Commission – would likely be taken more seriously by the companies concerned.

On a different note, we believe that the enforcement system in the Proposed CPC Reform should be improved by increasing the fines that national authorities may impose for an infringement of the Directives, and in particular of the UCPD and the Consumer Rights Directive. In our view, this could be achieved by linking the amount of the penalties to the turnover of the companies liable for infringing the UCPD and the Consumer Rights Directive, akin to the rules for fine-setting in cases of infringements of competition law and data protection law.[31]

Question 1.2.6.

To the best of our knowledge, in Italy the number of actions brought before civil and administrative courts against online providers' terms and conditions on the basis of consumer law has been relatively scarce. In contrast, in recent years the ICA has proved to be more active, and conducted several investigations on this matter pursuant to the UCTD and the UCPD.

For instance, in 2016 the ICA imposed a Euro 300,000 fine on Amazon EU Sàrl and Amazon Services Europe Sàrl for failing to provide or providing insufficient information to consumers purchasing online. In particular, according to the ICA, as regards direct sales, purchasers were not properly informed about the right to withdraw, the provision and terms of after-sale assistance and servi-

[30] Commission Notice on cooperation within the Network of Competition Authorities, OJ C 101/43.

[31] Regulation (EU) 2016/679 on the protection of natural persons in connection with the processing of personal data and the free movement of such data (the "General Data Protection Regulation;") willbecome effective on May 25, 2018. This Regulation will extend the scope of responsibilities for controllers and processors of personal data and enhance the enforcement regime to include, pursuant to Articles 83(5)-(6)6, fines of up to 4% of an organization's worldwide annual turnover.

ces, and the legal guarantee of conformity of goods. Concerning indirect sales (i.e., sales where Amazon merely acts as the online platform used by third-party sellers), according to the ICA, Amazon did not provide users with specific information on its role and obligations in these transactions, nor did it provide information on contracts and before- or after-sale assistance offered by third-parties.[32]

Moreover, in January 2017, the ICA found Samsung Electronics Italia S.p.A. ("*Samsung*") liable for two unfair commercial practices related to the promotional activities carried out for the sale of its devices, and imposed a Euro 3 million fine on it. According to the ICA, among other things, Samsung forced consumers – in order to benefit from the promotional price for the device they wanted to buy – to register onits platform "Samsung People" and to give consent to the use of their personal data for marketing purposes.[33]

In May 2017, the ICA imposed a Euro 3 million fine on WhatsApp for forcing users to accept in full its new Terms of Use (and specifically the provision to share their personal data with Facebook), by inducing them to believe that – without granting such consent – they would not have been able to continue to use the service anymore.[34]The same day, the ICA closed another investigation against WhatsApp, by ascertaining the unfair nature of some contractual clauses included in its Terms of Use, such as: particularly wide and general exclusions and limitations of responsibility in favor of WhatsApp; the possibility to unilaterally interrupt the service without reason or advance notice; as well as the general predominance in case of conflict of the English version of the contract over the Italian one (which was accepted by Italian users), without allowing the prevalence of the interpretation most favorable to the consumer, independently of the language in which the contractual clause is written.[35]

Finally, the Italian Administrative Court of First Instance (the "*TAR Lazio*") recently endorsed the appeals brought by Tripadvisor Italy S.r.l. and Tripadvisor

[32] See decision of March 9, 2016, No. 25911, case PS9353, *Amazon-Market place- Garanzia legale*.

[33] See decision of January 25, 2017, No. 26387, case PS10207, *Samsung- Marcato Riconoscimento Promozione*.

[34] See decision of May 11, 2017, No. 26597, case PS10601, *Whatsapp-Trasferimento dati a Facebook*.In July 2017, the ICA announced that it is investigating so-called "*influencer marketing*" practices carried out on social media (i.e., the posting on social networks of photos, videos, and comments by bloggers and influencers showing support or approval of specific brands, thus generating an advertising effect, without making clear to consumers the commercial intent of the communication). According to the ICA this practice may violate the prohibition of hidden advertising, which must be respected also in communications delivered through social networks. Therefore, the ICA addressed "moral suasion" requests to some of the main influencers and companies producing the branded goods displayed in the posts.*See* the press release, "*AGCM on Influencer Marketing: advertising must always be clearly recognizable*", Rome, July 24, 2017, http://www.agcm.it/en/newsroom/press-releases/2388-agcm-on-influencer-marketing-advertising-must-always-be-clearly-recognizable.html.

[35] ICA decision of May 11, 2017, No. 26596, case CV154, *Whatsapp-Clausolevessatorie*.

LLC (together, "*Tripadvisor*")[36] against an ICA decision that had imposed a Euro 500,000 fine against Tripadvisor for publishing misleading information about its reviews.[37]First, the TAR Lazio held that the type of information provided to consumers by Tripadvisor was coherent with the level of "expertise" that could reasonably be expected from an average internet user in 2014. In other words, it was legitimate to expect that the average internet user could understand the "risks" of an open website, without relying blindly on the reviews found therein. In any event, the TAR Lazio concluded that Tripadvisor had adequately informed consumers, stating on its website, that Tripadvisor cannot check the facts behind the reviews, thus allowing consumers to know in advance what kind of service they were being offered.

Question 1.2.7.

The issue of whether business-to-consumer ("*B2C*") rules should be extended to business-to-business ("*B2B*") relations has often been raised. Recently, the European Commission investigated this matter as part of the public consultation that led to the Fitness Check Report, concluding that – while some Member States already protect (to a certain degree) businesses against unfair contract terms and unfair commercial practices – views are still very divided, with many business associations and public authorities opposing the idea.[38]

With particular reference to the UCPD, since B2B relations are expressly excluded from its scope of application (see Recital 6), Member States in principle remain free to regulate such relations. Not surprisingly, most of them chose to implement the UCPD by keeping to its original scope.[39] Interestingly, Italy is among the seven Member States that opted (although to different extents) to apply the UCPD also to B2B relations.[40] Article 19(1) of the Italian Consumer Code (as amended by Article 7(2) of Decree-Law No. 1 of 24 January 2012,[41]

[36] See judgment of July 13, 2017, No. 9355. At the time of writing, the ICA brought an appeal against the TAR Lazio's decision, which is still pending before the Council of State.

[37] ICA decision of December 19, 2014, No. 25237, case PS9345, *Tripadvisor-False Recensioni On Line*.

[38] Fitness Check Report, p. 70.

[39] First Report on the application of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), COM(2013) 139 final, p. 9. As of 2016, seven Member States applied the UCP Directive also to B2B relations: *see* Guidance on the application of the Unfair Commercial Practices Directive, SWD(2016) 163 final, p. 10.

[40] *See* Guidance on the application of the Unfair Commercial Practices Directive, SWD(2016) 163 final, p. 10. As of 2016, such Member States were Austria, Sweden, Denmark, France, Germany, Italy and Belgium.

[41] Decree-Law No. 1 of 24 January 2012, *Disposizioni urgenti per la concorrenza, lo sviluppo delle infrastrutture e la competitività*, Italian Official Gazette General Series No.19 of 24 January 2012 – Ordinary Supplement No. 18.

converted with amendments into Law No. 27 of 24 March 2012),[42] extends the scope of application of the prohibition on unfair commercial practices to "*business to micro-enterprises*" relations.[43] "Micro-enterprises" are defined in Article 18(1)(d)*bis* in compliance with the European Commission Recommendation 2003/361/EC (the "*Commission Recommendation on SMEs*").[44]

The choice made by the Italian legislator must be welcomed, as it provides for a broader application of the rules on consumer protection, extending them to micro-enterprises, which, similar to consumers, are normally the weaker party in their relationship with traders. By the same token, it might be worth considering extending the scope of also the UCPD to micro-enterprises, in order to guarantee a uniform legal framework throughout the EU.

In fact, the lack of EU harmonization on this issue may be detrimental to businesses, by forcing them to adapt their behavior to different national legislation and undermining legal certainty. These costs are particularly burdensome for micro-enterprises, due to their limited dimensions. From this standpoint, it may be useful to envisage a uniform solution to this issue at the EU level.

Question 1.3.1.

Article 1(5) of the proposal for a Regulation on geo-blocking (the "*Proposed Geo-blocking Regulation*"),[45] in conjunction with Recital 10, expressly provides for the relationship between the Proposed Geo-blocking Regulation and other EU regulations, namely Regulation (EU) No. 1215/2012 (the "*Brussels I bis Regulation*")[46] and Regulation (EC) No 593/2008 (the "*Rome I Regulation*").[47]

[42] Law No. 27 of 24 March 2012, *Testo del decreto-legge 24 gennaio 2012, n. 1 (in Supplemento ordinario n. 18/L alla Gazzetta Ufficiale – Serie generale – n. 19 del 24 gennaio 2012), coordinato con la legge di conversione 24 marzo 2012, n. 27 (in questo stesso Supplemento ordinario alla pag. 1), recante: «Disposizioni urgenti per la concorrenza, lo sviluppo delle infrastrutture e la competitività»*, Italian Official Gazette General Series No. 71 of 24 March 2012 – Ordinary Supplement No. 53.

[43] Article 19(1) of the Italian Consumer Code states the following: "[t]*his Title shall apply to unfair business-to-consumer commercial practices before, during and after a commercial transaction in relation to a product as well as any unfair commercial practices between professionals and micro-enterprises. The protection of micro-enterprises from deceitful advertising and unlawful comparative advertising is explicitly guaranteed by Legislative Decree No. 145 of 2 August 2007*".

[44] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, OJ L 124/36.

[45] Proposal for a Regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC, COM(2016) 289 final.

[46] Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 351/1.

[47] Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations, OJ L 177/6.

In particular, Article 1(5) consists of two parts. The first part sets out a so-called safeguard clause stating that "[t]*his Regulation shall not affect acts of Union law concerning judicial cooperation in civil matters*", such as the Brussels I *bis* Regulation. This means that the Proposed Geo-blocking Regulation and the Brussels I *bis* Regulation are meant to be applied in parallel. As a consequence, the jurisdiction criteria laid down in the Brussels I *bis* Regulation, which will apply to cross-border disputes concerning B2C contracts, are:(i) the jurisdiction over consumer contracts (Articles 17 to 18), (ii) the special jurisdiction over contracts (Article 7(1)), and (iii) the prorogation of jurisdiction (Articles 19 and 25 to 26).

The second part of both Recital 10 and Article 1(5) provides that it cannot be implied that a trader is directing his activities to the consumer's Member State pursuant to Article 17(1)(c) of the Brussels I *bis* Regulation (thereby resulting in the application of Article 18 thereof)[48] for the sole fact that he is acting in accordance with the provisions of the Proposed Geo-blocking Regulation (*e.g.*, he allows consumers to access his website, regardless of the Member State where the consumer has its domicile, residence or nationality).

It must be noted that the Brussels I *bis* Regulation does not define the concept of activity directed to the Member State of the consumer's domicile contained in Article 17(1)(c). The Court of Justice of the European Union (the "*CJEU*") filled this gap in *Pammer*,[49] providing an autonomous interpretation of this concept.[50]In particular, the CJEU considered the trader's subjective intention to establish commercial relations with consumers from one or more other Member States, including the Member State of the consumer's domicile (the so-called "*voluntary element*"), and listed some objective elements, which may constitute evidence that the trader (whose activity is presented on his website, or on that of an intermediary) was minded to conclude a contract with these consumers.[51]Interestingly, the CJEU excluded the mere accessibility of the trader's or the intermediary's website in the Member State in which the consumer is domiciled.[52]

[48] Pursuant to Article 18 of the Brussels I bis Regulation, "*1. A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or, regardless of the domicile of the other party, in the courts for the place where the consumer is domiciled. // 2. Proceedings may be brought against a consumer by the other party to the contract only in the courts of the Member State in which the consumer is domiciled. // 3. This Article shall not affect the right to bring a counterclaim in the court in which, in accordance with this Section, the original claim is pending*".

[49] CJEU, December 7, 2010, joined cases C-585/08 and C-144/09, *Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG et al.*, ECLI:EU:C:2010:740.

[50] *Pammer*, para. 55; *Mühlleitner*, para. 28.

[51] *Pammer*, paras. 75-76 and 92.

[52] *Pammer*, para. 94, which also excluded the mention of an e-mail address and of other contact details, or of use of a language or a currency which are used in the Member State where the trader is established.

In light of the foregoing, the provision in Article 5(1) of the Proposed Geo-blocking Regulation shows the intention of the European Commission to exclude any interlink between the Proposed Geo-blocking Regulation and the Brussels I *bis* Regulation, as further confirmed by the fact that the Proposed Geo-blocking Regulation does not contain any specific rule on jurisdiction. However, the issue arises of how complying with the prohibition of geo-blocking practices, as set out in the Proposed Geo-blocking Regulation, affects the interpretation of the directed activity criterion under Article 17(1)(c) of the Brussels I *bis* Regulation, as developed by the CJEU in *Pammer*. Indeed, in light of the *Pammer* ruling the trader's obligation to supply goods and services in the EU without preventing access to his website to consumers domiciled in other Member States would arguably *per se* negate the trader's subjective intention to establish commercial relations with the Member State of the consumers' domicile.

The European Commission seems to consider this issue in the second part of Article 5(1) of the Proposed Geo-blocking Regulation, but does not advance a practical solution for this problem. In fact, national courts would have to ascertain the trader's intention to direct his activities to the Member State of the consumer's domicile on the basis of the objective factors developed in the CJEU case law, and would likely have to exclude such an intention whenever "*a trader is legally* coerced *to serve consumers in a certain state*".[53]

The possible entry into force of the Proposed Geo-blocking Regulation would therefore constitute an important opportunity for the CJEU to reconsider the well-established interpretation enshrined in the *Pammer* judgment.

1.4. Questions related to the collaborative economy

Question 1.4.1.

The emerging legal issues in the collaborative economy (also known as sharing economy) arena are mainly related to consumer law, competition law, labour law and tax law.

A very crucial and controversial point, not limited to the Italian jurisdiction, concerns the qualification of sharing economic platforms as information society service providers (i.e. mere intermediaries) under the E-Commerce Directive or professional operators subject to the relevant regulatory requirements. In this respect, it is worth noting that a request for preliminary ruling has been referred by the Juzgado Mercantil of Barcelona in the case *Asociación Profesional*

[53] See Von Hein, *Geo-blocking and the conflict of laws: ships that pass in the night?*, 31 May 2016, available at www.conflictoflaws.net, stating that "*any test aimed at determining his or her "state of mind" to do so necessarily becomes moot – which, on the other hand, may be a good opportunity for the CJEU to rethink its frequently criticized approach*".

*Elite Taxi v Uber Spain*and is currently pending before the Court of Justice of the European Union. Advocate General Szpunar, in his opinion released on May 11th, 2017, concluded that «*a service that connects, by means of mobile telephone software, potential passengers with drivers offering individual urban transport on demand, where the provider of the service exerts control over the key conditions governing the supply of transport made within that context, in particular the price, does not constitute an information society service [...] but constitutes a transport service*» (see also the Opinion of Advocate General Szpunar dated July 4th, 2017 in the *Uber France SARL* case, C-320/16).

Depending on the solution to this question, collaborative economy businesses like Uber may face a very different scenario from a legal standpoint, being at stake whether they are bound or not by the same requirements and obligations applying to the providers of 'traditional' services.

Although consumers generally benefit from collaborative economy services, some business models are facing different legal challenges in Italy. Some of these challenges were brought to light by the *Uber* saga, including a set of controversial courts' decisions.

First, in May 2015 the Court of Milan ordered the blocking of the *UberPop* service(allowing consumers to enter into contact with private car owners through an application) in the Italian territory. According to the Court of Milan, the performance of the *UberPop* service constituted an act of unfair competition and interfered with the cab public service offered by licensed taxi drivers. The Court of Milan stressed that this way Uber could obtain additional benefits compared to the latter, including by applying higher fares.

Secondly, on April 6th, 2017 the Court of Rome ordered the blocking of the *UberBlack* service (where, unlike *UberPop,* drivers hold a license for chauffeur driven car hire services) in the Italian territory through an interim injunction. The Court of Rome argued that the actual functioning of *UberBlack* was incompatible with the obligations set forth by the Law no. 21 of January 15th, 1992,regulatingtaxi and hire services. The injunction was eventually overturned on May 26th.

Against this background, in January 2016, a bill aimed at regulating collaborative economy services (*Regulation of digital platforms for the sharing of goods and services and the promotion of the sharing economy)* was introduced into Parliament.

In particular, the bill defines "collaborative economy" as the economy generated by the optimised and shared allocation of goods (albeit without any transfer of ownership rights) and services through digital platforms. The purpose of the bill is to create a level playing field for digital platforms offering collaborative economy services with a view to both fostering competition between innovative and traditional players and avoiding that the latter are negatively impacted by the rise of disruptive technologies.

Question 1.4.2.
Competition is definitely the most critical issue regarding the rise of collaborative economy in Italy. These business models are often felt as a threat to competition by traditional service providers that are subject to specific requirements laid down by the legal frameworks applying to the relevant categories of services. Yet, collaborative economy services may indeed foster competition, from a general standpoint. The concerns of traditional service providers arise from the lack of a level playing field between them and collaborative economy players. The use of digital platforms to deliver these services is often seen as a way to escape compliance with the relevant market access requirements – to which traditional service providers are subject – while competing *de facto* with the same. It is not by chance that the reasoning of courts, e.g. in the *Uber* saga, has focused on whether, on the basis of the relevant characteristics, traditional services and collaborative economy services were actually in competition and, thus, whether the performance of the latter amounted to unfair competition.

It is worth noting that the Italian Competition Authority (AGCM) has welcomed the development of collaborative models in light of the increasing of the degree of choice available to consumers and the high level of innovation.

Question 1.4.3.
As pointed out in the answers to Q.1.4.1 and Q.1.4.2, digital sharing economy platforms often operate in markets subject to certain access requirements. It becomes then crucial to determine whether these platforms enjoy the same legal status of the relevant traditional providers (and are subject to the same requirements), as suggested by Advocate General Szpunar, or should be qualified as information society service providers. With respect to taxi and hire services, for instance, the Law no. 21/1992 requires the possession of a license (in case of taxi service) or an authorization (in case of chauffeur driven car hire service) to be issued by the municipality where the service is operated to drivers that, in turn, meet certain requirements. Furthermore, the taxi and hire service is subject to certain limits. The goal behind this legal framework, that *per se* restricts competition, is to reconcile the individuals' "right to mobility" with consumers protection. Applying the same provisions to collaborative economy services will significantly impact, as the *UberPop* case brings to light, the business model of the "new players".

It is worth noting that the Italian Competition Authority has repeatedly urged Parliament to consider amending the legislation governing these services, which dates back to 1992. The Italian Competition Authority expressly suggested the "road" of soft regulation in order to preserve a dynamic competition in the market without affecting consumers protection, to facilitate the development of innovative platforms and to grant greater flexibility to taxi drivers.

Similar challenges may arise also in other markets having access requirements, including online apartments/room lease and rental services (e.g. the service provided by Airbnb) or home cooking services ("home restaurants").

Question 1.4.4.
Collaborative economy has blurred the distinction between traders and consumers since products and services are increasinglyoffered by subjects which act in their capacity as consumers and not traders or, in some cases, these services are directly offered by consumers to traders. This switch, from B2C to C2C (or in some cases C2B),raises difficulties in clearly determining the scope where consumer law applies.

It is worth noting that consumer protection has been significantly taken into account as one of the driving factor of the existing legislation on taxi and hire services in the *Uber* saga. The requirements which traditional service providers must abide by are then justified on the basis of the need of ensuring consumer protection and, in particular, the safety of passengers. Also the bill introduced to the Parliament with a view to regulating new collaborative economy platforms attaches special importance to consumer protection, as it expressly refer to the purposes to be pursued in accordance with Article 4, par. 1, no. 8 of Directive 2006/123/EU.

Question 1.4.5.
At the outset, it must be stressed that there is no specific definition of peer-to-peer services under the Italian law. In order to determine whether a subject offering peer-to-peer services does amount to a consumer or a trader, it is necessary first to consider the definition of "consumer" under the Italian Consumer Law. According to Section 3 of the Italian Consumer Code (Legislative Decree no. 206 of September 6th, 2005), consumers include «*any natural person who is acting for purposes which are outside his trade, business or profession*». Instead, the definition of "traders" (or "professionals") refers to «*any natural or legal person who is acting for purposes related to his trade, business or profession, or his intermediary*». It is worth mentioning that recently in the banking sector the Italian Bank Authority has tackled the activity of peer-to-peer lending. The Authority issued its rules on the collection of savings by subjects other than banks.

Question 1.4.6.
Online rating and review systems may definitely have an impact to remedy the lack of information and confidence by consumers in peer-to-peer services. Collaborative economy service providers are implementing such systems also with a view to allowing a degree of control over the performance of peer-to-peer

services and preserve higher standard of quality. Making legally binding the implementation of rating and reviewing systems may constitute an option to increase transparency and, generally speaking, consumer care.

However, these systems might give rise to legal issues to the extent digital platforms were deemed to exercise an editorial responsibility over the content of reviews. If so, they would most likely be excluded from the liability exemptions set forth by the E-Commerce Directive, by reason of the existence of a degree of control over third parties content.

2. Digital media

Question 2.1.

We are not aware of any actual repercussions of the judgment of 21 October 2015, *New Media Online GmbH v Bundeskommunikationssenat,* case C-347/14 in Italy.

In principle, this judgment may be read as implying that publishers must obtain from AGCOM the general authorization required for on-demand audiovisual media services for the parts of their websites that include short videos, pursuant to Article 22-bis of Legislative Decree no. 177 of 2005, the Consolidated Law on Audiovisual and Radio Media Services (CLARMS).

However, if the short videos concerned have already been broadcast through linear media, the exception laid down in Article 2(3) of AGCom decision 607/10/CONS might apply. That provision stipulates that no additional authorization is required for the provision of programs that have already been broadcast through linear media in keeping with the relevant authorization requirements.

It is worth mentioning that the non-linear audiovisual media services, albeit not subject to authorization requirements, must comply with the catalogue and investment requirements in favor of European works laid down by Article 4(1) of AGCom decision 66/09/CONS, as amended by AGCom decision 526/14/CONS.

Question 2.2.

One of the foremost concerns of the Digital single market strategy is ensuring a level playing field between traditional media providers and newcomers that offer competing services. In this connection, is thus necessary to redefine the subjective scope of the rules making up the audiovisual media services regulatory framework, so as to ensure that the regulatory burdens are allocated evenly, i.e. in a way that does not unduly distort competition in favor of certain categories of undertakings.

The other guiding principle for the regulation of the digital sector, including online platforms, is a strict necessity and proportionality assessment of the regulatory constraints placed upon the undertakings.

The proposal for the reform of the AVMS directive seems to take into account both those guiding principles. On the one hand, that proposal seeks to bring on demand services and other online audiovisual services within the scope of certain regulatory constraints applying to traditional broadcasters, notably with reference to the promotion of European Works, the protection of minors, and the ban on hate speech and incitement to hatred, which are going to be applicable to video-sharing platforms even though the latter do not enjoy full editorial control over their contents.

By the same token, in keeping with the principle of proportionality, the proposal seeks to relax the rules on advertising, product placement, and sponsored programs for traditional broadcasters, so as to take into account the developments that have occurred in the sector, which would otherwise make the current regulatory framework unduly burdensome for those players.

We believe that these reform perspectives go in the right direction, considering that in Italy we witness a regulatory gap in that respect. Besides, a fragmented regulatory framework at the national or local level would only create uncertainties for users and providers, thus undermining the functioning of the digital single market.

Nonetheless, it seems most appropriate to keep regulatory intervention at the EU level (rather than at the national or local level) and to limit the enactment of further regulatory constraints to instances where they really are necessary and proportionate, on the basis of a cost-benefit analysis.

Another open issue is whether special rules are needed to regulate the relationship between platforms and undertakings, notably small and medium-sized ones, which may suffer from a significant unbalance of bargaining powers. Notably, it is worth considering the introduction of codes of conduct on issues such as transparency, data portability, access to dispute resolution, so as to ensure the functioning of the digital single market in keeping with the principles of necessity and proportionality.

Question 2.3.

To our best knowledge, the country-of-origin principle has not given rise to particular concern as regards implementation in Italy, insofar as the Italian rules mostly mirror those of the AVMS.

In particular, Section 1-bis(1)-(5) CLARMS reflects *verbatim*, except for the necessary linguistic adjustments, the rules on jurisdiction laid down in Article 2 AVMSD. Section 1-bis(6) CLARMS, instead, has no equivalent in the AVMSD. That provision, however, appears largely redundant, in that it merely reaffirms the principle that media service providers subject to Italian jurisdiction must comply with Italian rules, regardless of the Member State they "belong to".

We are not aware of any lawsuit that concerns the application of those rules to specific cases or of any non-EU providers targeting the Italian audience.

Question 2.4.

It is certainly desirable that, in any future EU interventions, the independence of the NRA in the AMS sector will be considered a prerequisite for the compliance of national legislation with EU law. It would also be a step forward if the principle laid down by recital no. 13 of Directive 2009/140/EC, according to which national legislative bodies are "unsuited to act as a national regulatory authority", were expressly extended to the AMS sector.

The implementation of those principles in Italy poses certain unique challenges. Although Law 249/1997 stipulates that AGCom is an "independent authority", its actual independence from political parties and operators subject to its oversight have been contested.

To avoid conflicts of interest with the government, political parties and industry, the law provides that AGCOM president and commissioners cannot hold other offices at the same time. There is also a cooling-off period of four years, during which the president and the commissioners cannot have a working relationship with companies active in AGCOM's field of competence. Those rules did not prevent a former AGCOM Commissioner to take up an appointment as Under-secretary of State for Defence, following the conclusion of his tenure at AGCOM.

Moreover, no rules are in place having regard to the occupations and political affiliations that AGCOM President and Commissioners held prior to their appointment to that regulatory body, except that they have a recognized expertise in the sector (but, in practice, also that requirement is not always respected, having the AGCOM's formation witnessed even the presence of... medical doctors). Since AGCOM'sPresident and Commissioners are elected by the Parliament, they are usually linked to specific political parties. In particular, two are usually the expression of the ruling political majority and two of the opposition while the fifth one (the President) is appointed by the Prime Minister (head of government) in agreement with the Minister of Economic Development following approval of the competent parliamentary committees (acting by a majority of two-thirds).

The influence of politics on AGCOM therefore materializes as early as in the phase of appointment of its board members. This is concerning, since AGCOM is entrusted also with the enforcement of the rules on political communication (*par condicio*).

Question 2.5.
Most AVMSD provisions have been transposed verbatim into the CLARMS. There are, however, two specificities of the Italian media and regulatory landscape that have given rise to litigation in courts and debate in academic and political circles.

One of them is the rule, laid down in Article 38(5) CLARMS, whereby advertising by pay-tv broadcasters is subject to a hourly limit of 16% in 2010, 14% in 2011, and 12% from 2012 onwards. In its 2012 inquiry into the advertising sector (attachment A to AGCom Decision no. 551/12/CONS), AGCom noted that those asymmetrical advertising limits for pay-tv broadcasters could further increase the concentration of the advertising market to the advantage of the dominant player (Fininvest/Mediaset), insofar as those stricter limits mainly affected the only competitor (Sky) that had been able to increase its market share over the previous years.

Sky Italia thus violated the asymmetrical quantitative limit for pay-tv broadcasters and challenged AGCom's infringement decisions before the Latium Regional Administrative Court, which in turn referred the matter to the Court of Justice of the European Union for a Preliminary Ruling. In its judgment of 18 July 2013, *Sky Italia Srl v Autorità per le Garanzie nelle Comunicazioni*, Case C-234/12, the Second Chamber of the ECJ ruled that Article 4(1) of the AVMS Directive as well as the principle of equal treatment and Article 56 TFEU must be interpreted as not precluding, in principle, a national rule, such as that at issue in the main proceedings, which lays down shorter hourly television advertising limits for pay-TV broadcasters than those set for free-to-air broadcasters. However, the ECJ also stated that it was for the referring court to determine whether those asymmetrical rules were in keeping with the principle of proportionality.

Following the ECJ's preliminary ruling, the Latium Regional Administrative Court referred a preliminary question of constitutional legitimacy to the Constitutional Court. The latter, in its judgment no. 210 of 2015 ruled that the differential quantitative limits for pay-tv operators, which were introduced by the Italian Council of Ministers in the context of the implementation process of the AVMS Directive in the absence of a specific authorization by the Parliament, was in keeping with Article 76 of the Constitution, regulating the delegation of legislative powers by the Parliament to the Council of Ministers. The Constitutional Court, instead, dismissed as inadmissible the constitutional challenge based on the violation of the principle of equality laid down in Article 3 of the Constitution, insofar as that issue had been already addressed by the ECJ in its judgment of July 2013.

The case, thus, was remanded to the Latium Regional Administrative Court, which must still determine whether the differential advertising limits for pay-tv

operators are in keeping with the principle of proportionality, i.e. that they do not go beyond what is necessary to protect consumers against an excessive exposure to advertising. That decision was entrusted to a different chamber of that Court. Nonetheless, to date, that Chamber has not yet scheduled a hearing for the case.

Another specificity of the Italian media landscape is the particularly rich offer of audiovisual media services by Italy's public service media operator RAI. Those contents are accessible by satellite either through the purchase of a decoder from Tivùsat, a company controlled by RAI, or through decoders distributed by Sky Italia, a pay-tv satellite operator.

The issue has arisen whether RAI, which provides its programs free of charge to Tivùsat, may charge Sky Italia for the provision of the same contents. The Latium Regional Administrative Tribunal (judgment no 6320 of 11 July 2012) and the Council of Statehave taken the view that access to RAI's contents through Sky Italia's decoders upholds the principle of universality of public services, considering that Sky Italia does not charge any additional fee for access to RAI's programs.

However, in Decision no. 128/15/CONS, AGCom took the view that, unlike TivùSat, Sky Italia has a self-interest in distributing RAI's programs through its decoders as it also distributes pay-tv services. Hence, RAI is entitled to charge Sky Italia for the distribution of its proprietary contents.

Question 2.6.

Targeted advertising is a recent practice in Italy, that is steadily gaining ground. According to press releases, targeted advertising has been employed by Italy's main pay-tv, that is able to convey targeted advertising to different types of users, in line with a broader trend that is already prominent on the internet (Google and Facebook). Thanks to this system, known as AdSmart, different categories of users watching the same linear program will view personalized advertising during the advertising breaks.

As this phenomenon is fairly recent, it has not been addressed by the media regulator (AGCOM). In all fairness, the legal classification of targeted advertising against the background of the AVMS Directive appears problematic. Indeed, targeted advertising cannot be regarded as a linear broadcast, as it is downloaded and stored in the decoder's hard drive. Equally, it cannot be considered as an on-demand broadcast, as the users do not willingly request that particular audiovisual content, nor they choose the time it is displayed.

In particular, the linear program consists only of the editorial contents that form part of the satellite feed, whereas targeted advertising is stored into the decoder and thereby combined with the satellite feed, thus giving rise to a "hybrid content" that has no clear legal classification and is not subject to a prior authorization regime.

Having said that, it seems undisputable that the targeted advertising spots that replace the ones incorporated in the satellite feed are subject to the general rules applicable to advertising spots, notably as to the programs in the context of which they can or cannot be inserted and the frequency of the advertising breaks. Moreover, targeted advertising must surely comply with the general principles governing audiovisual commercial communications and notably the rules on the protection of minors. Equally, they are subjects to restrictions if they concerns certain products or services (e.g. tobacco, medicines available under prescription and medical treatments, alcoholic beverages).

We further speculate that targeted advertising must comply with the more detailed rules on advertising laid down in the Co-regulatory Code TV and minors. Notably, between 4 pm and 7 pm targeted advertising cannot concern alcoholic beverages, premium telephone and entertainment services, birth control methods (except for public awareness campaigns). Between 7 am and 11 pm targeted advertising cannot convey PG-14 movie trailers. Furthermore, PG-18 movie trailers cannot be displayed at any time.

Also advertising quantitative limits seem applicable to targeted advertising. It could be objected that targeted advertising spots should not be subject to those rules, as they form no part of the linear broadcast. However, as the purpose of the rules on quantitative limits is to protect viewers from an excessive exposure to advertising, it seems that those rules should also apply to targeted advertising spots, considering that they merely differs from the advertising sports incorporated in the linear broadcast as regards its technical conveyance means and that the viewer is completely unaware of the replacement of certain spots with personalized ones, as the latter are not preceded or followed by any type of notice to that effect.

According to the information currently available, targeted advertising in Italy will be differentiated on the basis of regional clusters. This, however, seems to possible consistency issues with Section 38(10) CLARMS, according to which local advertising is reserved for local broadcasters, whilst nation-wide broadcasters, including the public service media operator, must broadcast advertising at the same time and with the same content in all the regions concerned.

Finally, the Italian Data Protection Authority issued a decision on 13 July 2016 (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5408313), ruling that the provision of targeted advertising is in keeping with the Italian Data Protection Code (legislative decree no. 196 of 30 June 2003), as long as the users are duly informed, as per Section 13 thereof, of the purpose of data processing (i.e. profiling-based marketing), the safeguards in place to ensure that data are anonymized and processed only in aggregate form, and the possibility to exercise their statutory rights to information and transparency.

Question 2.7.
Under Italian law, the keystone provision regulating the copyright aspects of satellite broadcasting is Section 16-bis of the Italian Copyright Law, which was added to Law 22 April 1941, no 633 by Section 2(1) of Legislative Decree 23 October 1996, no. 581.

From the *travaux préparatoires* of Legislative Decree 23 October 1996, no. 581, it is apparent that the Italian Government enacted the above provision to transpose into Italian law Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission.

Section 16-bis of the Italian Copyright Law is still in force and has not been amended since its enactment.

In view of the congruencies with the contents of Council Directive 93/83/EEC, it can thus be argued that the special regime for copyright licensing set out therein is still relevant in Italy. However, we are not aware of that regime being applied to media other than satellite and cable, let alone the internet.

Question 2.8.
Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market, the so-called "Portability Regulation",seeks to harmonize national rules in respect of portability of on-line portable services (hereinafter also the "online services"). "Portability" means the possibility for a subscriber to a certain online portable service (whether or not offered on a standalone basis), who is resident in a particular Member State, to access such service also from a different Member State, during his or her temporary presence in such latter State.

The harmonization of on-line portability is an objective that differs from that of harmonizing the right of communication to the public via internet, on which the UE legislature has been working in the last months, as shown by the Commission's Proposal for a Regulation of the European Parliament and of the Council laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organizations and retransmissions of television and radio programmes (COM(2016)594).

In Italy as well as in other Member States, the main stumbling block to cross-border portability of digital contents is, arguably, the territorial application of copyright law. The Portability Regulation apparently takes that factor into account under recital 4, which acknowledges that "the rights for the transmission of content protected by copyright or related rights, such as audiovisual works, are often licensed on a territorial basis, as well as from the fact that providers of online content services might choose to serve specific markets only ".

To overcome that obstacle, the Portability Regulation resorts to a legal fiction, whereby the provision of an online content service under this Regulation to a subscriber who is temporarily present in a Member State, as well as the access to and the use of that service by the subscriber, shall be deemed to occur solely in the subscriber's Member State of residence (Article 4 of the Portability Regulation).

The Portability Regulation also recognizes the validity of the territorial limitations commonly provided under the agreements between right-holders and providers of portable online services. By the same token, the Portability Regulation expressly recognizes the service provider's freedom to target only certain territories and markets (see recitals 4, 5, 10, and 12). However, the territorial limitations contained in the agreements between right-holders and providers of online services cannot affect the subscribers' right to receive and view such services when they are temporary located in other EU Member States.

The Portability Regulation lays down specific rules on the verification of the subscriber's Member State of residence (Article 5). The provider is entitled to verify the subscriber's Member State of residence by using no more than two of the means of verification exhaustively listed in Article 5(1) and must "ensure that the means used are reasonable, proportionate and effective". Should the service provider have reasonable doubts about the subscriber's Member State of residence in the course of a contract, it may repeat the verification process.

These arrangements seek to strike a balance between the legitimate expectation of the providers to verify the subscriber's State of residence and of the users concerns as to the processing of their personal data. Indeed, recital 28 of the Portability Regulation adds that IP address checks performed under this Regulation should be conducted in accordance with Directives 2002/58/EC and 95/46/EC, which is going to be repealed and replaced, with effect from 25 May 2018, by Regulation (EU) 2016/679 (the General Data Protection Regulation).

3. Digital infrastructures

Question 3.1.

Prior to the adoption of Regulation (EU) 2015/2120, there were not rules on net neutrality applicable in the Italian legal order. However, before the adoption of said Regulation, in 2014, a bill on net neutrality named "Rules on supply of Internet services for the protection of the competition and the freedom of user access" (also known as "DDL Quintarelli) was drafted. At present, it has not been passed into law by the Parliament yet and a debate has recently come up with respect to the compatibility of some provisions of the bill with EU law.

With respect to zero rating, as of the entry into force of the Regulation, the Italian Communications Authority (AGCOM) has carried out a comprehensive assessment on the websites of the most important service providers and,

particularly, on the economic and technical terms and conditions applied by the same. AGCOM has then run another assessment after the release of the BEREC Guidelines, in particular on Mobile Network Operators (MNO) and Mobile Virtual Network Operators (MVNO) with a view to exploring the types of zero-rated services offered, the traffic management measures adopted by these operators, the relevant data caps and the measures to ensure transparency and for the management of customer service. Zero-rated services include, among others, music streaming, video/IPTV streaming, social media, vocal services and SMS, e-reading, highlights of sport events, storage cloud services.

As result of this investigation, AGCOM has served a telecommunication provider with a cease and desist order because of unfair practises which discriminated the traffic on the Internet (123/17/CONS).

Question 3.2.

The development of a new single market of telecommunications networks should be a priority for the achievement of the objectives of the Digital Single Market Strategy. The adoption of the new EU telecoms package will constitute another step towards such aim.

On March 3rd, 2015, the Italian Government approved the Italian Strategy for high-speed broadband ensuring: a) a future-proof telecommunications infrastructure bringing connectivity with a minimum of 100Mbps covering up to 85% of the population by 2020; b) coverage of at least 30Mbps to all citizens. Moreover, the Government will promote the development of this project through a) simplification of the regulatory framework; b) creation of new growth drivers; c) tax incentives; d) reduction of installation costs. Within such project, Italy adopted a national state aid scheme, approved by the EU Commission in June 2016, to support ultra-broadband in market failure areas.

The project is coordinated by the President of the Council of Ministers through the Committee for the spread of high-speed broadband (COBUL). Furthermore, the Ministry of Economic Developments will be competent to implement the measures identified by the Committee for the application of the national strategy, including use of its in-house company Infratel Italy SpA, coordinating also the activities of public and private operators involved. Moreover, in 2017, a 5G trial has been launched in five cities: Milan, Prato, L'Aquila, Bari and Matera.

Question 3.3.

The most important legal issue on spectrum management relates to the transition of the 700 MHz band to the TLC sector. As it is well knows, the 700 MHz band (694-790 MHz) is predominantly occupied by TV channels (that will be reallo-

cated to sub 700 MHz bands) but has now to be converted to mobile (namely wireless broadband) in order to allow the introduction of 5G in Europe. According to the European Commission, this transition should be completed by June 30th, 2020 at the latest. Italy has reported some difficulties to meet the said deadline, most of which are due to the 20 year-term licenses granted in 2012 to broadcasters, that will be compensated accordingly. The deadline can however be postponed to June 30th, 2022 on the basis of justified reasons.

Question 3.4.
Independence of NRAs has been a long time debated issue in Italy, since under Italian law the members of said authorities are generally elected by the Parliament. This mechanism creates an inherent connection between political parties and the members of NRAs. Nonetheless, the law mitigates the importance of this link by generally requiring members of NRAs being chosen among candidates having a specific expertise and independence.

4. Data in the digital economy

Question 4.1.
To date, there are no specific legislative proposals or executive measures that have been enacted in Italy as a result of the General Data Protection Regulation (the "*GDPR*")[54]. However, over the last several months, the Italian Data Protection Authority (the "*IDPA*") has started publishing documents to clarify the interpretation of the most innovative provisions of the GDPR, as well as to indicate national provisions issued by the IDPA that will remain applicable after May 25, 2018 and future measures that the IDPA plans to adopt.[55]

Notably, on April 28, 2017, the IDPA published guidelines that, among other things, list certain measures that the IDPA plans to adopt in the coming months. For instance, regarding the notification of personal data breaches to the supervisory authority (which applies to all data controllers under Article 23 of the GDPR, as opposed to under current Italian legislation where it applies only to certain types of data controllers), the IDPA clarified that it will adapt the current notification forms in order to make them usable for all kinds of controllers. In a note published on its website on July 18, 2017, the IDPA also clarified that the Italian legislature has not yet established the identity of certification bodies

[54] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1.
[55] The IDPA has included in its institutional website a section specifically concerning the GDPR (www.garanteprivacy.it/regolamentoue), which is being populated with information and documentation.

pursuant to Article 43 of the GDPR, nor have the "additional requirements" for accrediting certification bodies or the certification criteria been defined. The IDPA is currently working, together with the data protection authorities of other Member States, to define a common framework for this issue.

Question 4.2.

In part due to the increase in non-compliance fines in the GDPR (as compared to the fines provided for in the Italian Data Protection Code),[56] the GDPR has prompted Italian businesses to pay unprecedented attention to data protection issues. Businesses in Italy are gradually becoming more and more aware that the GDPR's obligations are not simply limited to additional paperwork (such as updating information notices or deeds of appointment of third parties as data processors), because, in certain cases, they are capable of imposing structural modifications to the personal data processing mechanisms. Accordingly, several Italian businesses – especially large ones operating in different countries – have started to plan and implement management models of processes that involve the handling of personal data, based on a detailed analysis of the data processing as well as the connected risks. Furthermore, certain provisions of the GDPR create obligations that did not previously exist in Italy. For instance, the data protection impact assessment (Article 35 of the GDPR) is a new addition to the Italian framework that will replace the "prior checking" that the IDPA currently carries out pursuant to Article 17 of the Italian Data Protection Code.[57]The designation of a data protection officer (Articles 37 onwards) is also a new addition to the Italian framework. Businesses in Italy are establishing how to incorporate this new role within their organizations' structure and governance arrange-

[56] Legislative Decree No. 196 of 30 June 2003, *Codice in materia di protezionedeidatipersonali*, Italian Official Gazette General Series No. 174 of 29 July 2003 – Ordinary Supplement No. 123.

[57] Pursuant to Article 17 of the Italian Data Protection Code, processing activities likely to raise specific risks for the rights and freedoms of data subjects are only allowed in accordance with measures and precautions laid down by the IDPA, which is required to carry out a check before the beginning of that processing (the so called "prior checking"). By contrast, pursuant to Article 35 of the GDPR, with regard to processing operations likely to result in a high risk to the rights and freedoms of natural persons, it is on the data controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal dataIn other words, based on Article 35 of the GDPRit is the responsibility of the data controller to:(i) assess the risks to the rights and freedoms of data subjects, and (ii) identify the measures envisaged to reduce those risks to an acceptable level. Consultation with the supervisory authority is necessary only in cases where the data controller cannot find sufficient measures (i.e. when the residual risks are still high). However, pursuant to Article 36(5) of the GDPR, Member States are entitled to impose *ex ante* authorization obligations on public interest grounds.

ments, particularly in light of Article 29 of the Working Party's Guidelines on Data Protection Officers.[58]

Question 4.3.

The debate in Italy on the internet of things ("IoT"), smart cities, machine-to-machine generated data and automated cars mainly focuses on issues relating to the large amount of data generated by the functioning of these services ("Big Data").[59]

Notably, on May 30, 2017, the IDPA, the Italian Communications Authority (the "ICOA") and the ICA (together, the "*Authorities*") started a joint sector inquiry, with a view to addressing the potential risks associated with the use of Big Data andto outlining a regulatory framework aimed at ensuring the protection of consumers, competition in the digital economy markets and pluralism in the digital ecosystem.[60]As these Authorities noted, the use of Big Data can pose risks for the privacy of individuals, especially in relation to the ownership and protection of personal data, in light of the fact that modern analysis techniques often allow the re-identification of individuals through information that is allegedly anonymous. Additionally, Big Data contains the potential for increasingly more accurate human profiling, thus giving rise to the risk of discrimination and potential restrictions on the freedom of individual. The Authorities also highlighted the risk that profiling activities relying on Big Data could adversely affect market competition, net neutrality (thus access to and use of services) and information pluralism.

With specific reference to IoT, on March 26, 2015, the IDPA launched a public consultation (the results of which have not yet been published) aimed at identifying the risks to personal data protection connected with the use of technologies that allow the interconnection (and interaction) of objects and IT systems. The IDPA also took part in the 2016 Global Privacy Enforcement Network (GPEN) Sweep on the "Internet of Things."[61]

[58] *See* the Guidelines on Data Protection Officers ('DPOs') adopted on December 13, 2016 as last revised and adopted on April 5, 2017, WP 243 rev.01, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44100. The scope of the addressees of the provisions on data protection officers is still unclear because Member State law may provide for cases (in addition to those listed in Article 37(4) of the GDPR) where designation of a data protection officer is mandatory.

[59] The Cambridge Dictionary defines "Big Data" as very large sets of data that are produced by people using the internet and that can only be stored, understood and used with the help of special tools and methods. As is well-known, the most common definition of Big Data is based on the "3Vs" model (volume, velocity and variety).

[60] ICA decision of May 30, 2017, No. 26620, case IC53, *Big Data*.

[61] In this context, the IDPA analyzed different types of devices, focusing primarily on home automation, in order to identify flaws in compliance with personal data protection laws by the companies that operate in this sector.

Question 4.4.

The CJEU did not provide a clear rule to balance the various fundamental rights at stake when individuals exercise their "right to be forgotten", under which a search engine operator, in its role as personal data controller, must remove search results that are in breach of data protection rules. Unsurprisingly, this has led to several claims being brought before the IDPA (and, in the appeal phase, before Italian courts). As noted in the IDPA's yearly report issued in June 2017, claims involving the exercise of the right to be forgotten increased from 24% to 31% in 2016[62]. However, Italian precedents do not yet demonstrate a clear rule regarding the criteria for striking the balance between the individual's right to data protection and the other interests at stake. Italian authorities have adopted a case-by-case approach, mostly taking into account the gravity of the facts relating to the data subjects, on the one hand, and the length of the time that has passed since the occurrence of such facts, on the other hand.[63]

Regarding the breadth of the rights of data subjects, a debate exists in Italy as to what extent, in addition to de-listing, data subjects can request that information be erased from on-line newspaper archives.[64]

[62] IDPA's Annual Report 2016, available at http://194.242.234.211/documents/10160/0/relazione+annual+2016+-+Il+testo.

[63] Specifically, under this approach, the more serious the facts (thereby justifying the public's interest in such facts), the less relevant the length of the time that has passed since the facts occurred. See, for instance, the IDPA decision of March 31, 2016, doc. web No. 4988654, available at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb /4988654, whereby the IDPA rejected the de-listing request from the Google search engine of an individual who was criminally convicted in relation to conducts amounting to terrorism carried out in the 1970s and 1980s, notwithstanding the fact that the individual had finished serving his sentence in 2009. When criminal cases are at issue, whether the proceeding has come to a conclusion may be relevant in determining if the information should be considered outdated. However, in a case decided by the Italian Supreme Court (the "Corte di Cassazione") in its judgment of June 24, 2016, No. 13161, notwithstanding that a criminal proceeding had not yet concluded, the right to be forgotten of the data subjects was successfully claimed based on the argument that no significant case developments had occurred for several years.

[64] In this respect and with reference to information that is correct but outdated, the Corte di Cassazione, in its aforementioned judgment No. 13161/2016, held that an on-line newspaper had to erase the information from its archive because, notwithstanding the de-listing, the information was easily accessible to the public. Conversely, in its judgment on January 24, 2017, No. 1303, the Court of Rome held that the right to de-listing does not include the right to have information erased from the archive of an on-line newspaper, which provides news access to those who are specifically seeking out that information.

MALTA

Odette Vella[*] • Grace Stivala[**]
David Mifsud[***] • Antoine Grima[****]
Kevin Aquilina[*****] • Francis Zammit Dimech[******]
Pierre Cassar[*******] • Edward Woods[********]
Saviour Cachia[*********] • Ian Deguara[**********][1]

1. Internal Market and electronic commerce : Internet and e-commerce

1.1. Electronic Commerce, liability of Internet intermediaries

Question 1.1.1.

The E-Commerce Directive has been transposed by the Electronic Commerce Act (chapter 426 of the laws of Malta) dealing with *inter alia* liability of information society service providers. The Electronic Commerce Act transposes the

* Director (Information, Education and Research).
** Director (Enforcement), Office for Consumer Affairs, Malta Competition and Consumer Affairs Authority (MCCAA).
*** Director – Quality Assurance and Licencing at Malta Tourism Authority.
**** Assistant Lecturer, University of Malta.
***** Professor and Dean of the Faculty of Laws of the University of Malta; Head of the Department of Media, Communications and Technology Law; formerly (2000-2009) Chief Executive Officer of the Maltese audiovisual broadcasting regulator, the Broadcasting Authority.
****** Member of Parliament; visiting Senior Lecturer Media, Communications & Technology Law, Faculty of Laws, University of Malta.
******* former Chief Executive, Broadcasting Authority.
******** Chairman, Malta Communications Authority.
********* Information and Data Protection Commissioner.
********** Director – Operations and Programme Implementation, from the Office of the Information and Data Protection Commissioner.
[1] Unsuccessful attempts were made to hold discussions with the following: The current CEO of the Broadcasting Authority; National experts on Intellectual Property; A representative of the Ministry for the Economy, Investment and Small Business (MEIB); Transport Malta.

parent Directive (in Articles 19 – 22) and no further in depth engagement with the issues raised has been undertaken in Malta or by the Maltese courts, to the best of this author's knowledge.

To the best of this author's knowledge, there is no case-law in Malta concerning intermediary liability.

Question 1.1.2.
Yes, in this author's opinion the test is reasonable. The main fault with the test is perhaps one that cannot be fully overcome: that it still leaves considerable uncertainty as to how a national judge should apply aspects of the test (e.g. applying terms such as 'neutral host', 'active or passive role', 'diligent economic operator' etc.) to the factual case before him, in particular when the activities of the intermediary (e.g. Google or eBay) are varied and the assessment of such may therefore not be consistent across the different Member States, even in situations where the facts are essentially equivalent or even identical. There is also some vagueness as to the extent to which technical processes may constitute an indication of 'assistance' as a result of which the intermediary 'must be considered not to have taken a neutral position' (e.g. the promotion of offers such as 'enhanced' listings and email 'push' services).

Question 1.1.3.
This author considers the regime of notice-and-take-down to be appropriate, if not always sufficient. However, take-down should not be automatic, as that would impact negatively on the fundamental right to freedom of speech. This issue should ideally be regulated in a more detailed fashion at EU level.

Other appropriate solutions could include an obligation of some extent of pro-active filtering; for e.g. in the case of hate speech on social networks such as Facebook.

Question 1.1.4.
To the best of this author's knowledge, injunctions have never been considered/imposed in Malta/by a Maltese court.

1.2. Consumer protection in relation to the Internet and E-Commerce, Internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.
Complaints are normally brought before the Consumer Claims Tribunal (CCT). The CCT is the mechanism set up with the objective of resolving disputes between consumers and traders when conciliation has not resulted in an agreement on all

issues in dispute between a consumer and a trader. For further information see http://mccaa.org.mt/en/consumer-claims-tribunal. On the Consumer Claims Tribunal see also Odette Vella. 2015. The Consumer Claims Tribunal. Times of Malta. Available at https://www.timesofmalta.com/articles/view/20150920/consumer-affairs/The-Consumer-Claims-Tribunal.585131

Information on guarantees and returns in Malta is available here: http://europa.eu/youreurope/citizens/consumers/shopping/guarantees-returns/malta/index_en.htm

A number of cases have been brought before the CCT in the context of contractual guarantees on the purchase of second-hand cars. While these decisions generally provide scant legal discussion, generally the position of the arbiter has been that second-hand cars are sold 'tale quale', excluding latent defects; it is therefore the responsibility of the buyer to engage competent persons to examine all aspects of the vehicle prior to purchase, all the more so when it's an old vehicle. Hence remedies in such situations were generally declined. (see for e.g. Lautier v Ventur Motor Center Co. Ltd. Consumer Claims Tribunal. CCT 324/12/GB. 15 May 2013; and Mizzi vs Anthony Baldacchino/ABS Auto Dealer. Consumer Claims Tribunal. CCT/121/14/S. 25 June 2015.)

However, it does not result that these decisions are instructive from a digital market perspective.

Question 1.2.2.
This author was not able to identify any national perspective on this issue. No response was forthcoming from the government Ministry responsible for this proposed EU Directive.

Question 1.2.3.
This author was not able to identify any national perspective on this issue. No response was forthcoming from the government Ministry responsible for this proposed EU Directive.

Question 1.2.4.
The effect of the harmonised rules should be beneficial on the enforcement of EU consumer protection legislation. Harmonisation helps enforcement, and facilitates coordination between consumer agencies and NGOs, and European consumer centres.

Question 1.2.5.
Current EU consumer protection law suffers from limitations in terms of enforcement against the intermediary online platform itself, rather than the remoter possibility of enforcing against the individual trader utilising the platform:

For e.g., if one were to consider the possibility of finding an online platform liable under the e-Commerce Directive 2000/31/EC provisions on intermediary liability: should an administrative enforcer provide notice to the online auction site, this constitutes knowledge; but there may be limitations with engaging the liability of the host as consumer legislation may be directed at enforcing against primary infringers (hence, no underlying liability of the online platform). This author concurs with Riefa (2015) 221 who states:

> "It is possible to envisage an even wider liability regime, forcing intermediaries to also ensure against the use of unfair commercial practices or unfair terms on their platforms. This is not yet possible and some amendments to legislation are necessary to make it a reality, but it could provide a viable solution in the future." (Riefa (2015) 221).

As regards the possibility of injunctions against intermediaries (enforcement powers/enforcement orders), the same author suggests:

> "There is therefore a gap in legislation in order to offer a means of protecting consumers pre-emptively and enabling enforcers and courts to stop practices perpetrated via online auction platforms. Such limitations do not apply in matters relating to intellectual property, since the enabling legislation does contain means to obtain injunctions against the third parties enabling the litigious activity." (Riefa (2015) 202).

As regards enforcement powers, in Malta, "Further to investigations and administrative proceedings by the Enforcement Directorate, the Director General of the Office for Consumer Affairs issues public warning statements on traders who fail to comply." (source: MCCAA website) Further to investigations conducted either ex officio or upon a complaint of an interested party, the Director General (Consumer Affairs) may issue an administrative decision finding an infringement. This can be issued simultaneously with a compliance order and with the imposition of fines. In addition, the Consumer Affairs Act (Laws of Malta – chapter 378) also endows the Director General with *locus standi* in the prosecution of offences before the Court of Magistrates for an offence under the Act or any regulation made thereunder. In such case it is the Director General or any other Officer authorised to act in her stead who shall conduct the prosecution.

The European Commission Fitness Check of consumer and marketing law and the evaluation of the Consumer Rights Directive (29.05.2017): http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=59332

"In addition, the evaluation shows targeted legislative changes to address certain identified shortcomings of the Directives could be beneficial. For example,

in light of recent developments in the digital economy, one such change could be enhancing the transparency of online platforms."

Question 1.2.6.
No (not to the best of this author's knowledge).

1.2.7.
B2C is very limited in scope. In Malta we have many small businesses and therefore in certain circumstances (inequality in bargaining power) it would be desirable if the rules were expanded to include B2B.

1.3. Geo-blocking

Question 1.3.
The author has not be able to identify a national perspective on this question.

The Council General approach on the draft regulation addressing geo-blocking (28 November 2016) includes the following text:

> 'This Regulation should be without prejudice to acts of Union law concerning judicial cooperation in civil matters, notably the provisions on the law applicable to contractual obligations and on court jurisdiction set out in Regulations (EC) No 593/2008 of the European Parliament and of the Council (Rome I) and (EU) 1215/2012 of the European Parliament and of the Council (Brussels). In particular, *the mere fact that a trader complies with the provisions of this Regulation should not be construed as implying that he directs his activities to the consumer's Member State within the meaning of Article 6(1)(b) of Regulation (EC) No 593/2008, and of Article 17(1)(c) of Regulation (EU) 1215/2012.* Therefore, the mere fact that the trader does not block or limit access to his or her online interface for customers from another Member State or does not apply different general conditions of access in the cases laid down in this Regulation or does not apply different conditions for payment transactions within the range of payment means he accepts, should not be considered, on its own, as directing the traders activities into the Member State of the consumer, for the purpose of the determination of the applicable law and jurisdiction. (recital (10) author's italics).'

This is also specifically laid down in the Council general approach text at Article 1(5):

> 'This Regulation shall be without prejudice to Union law concerning judicial cooperation in civil matters. Compliance with this Regulation shall not be construed as implying that a trader directs his or her activities to the Member State where the consumer has the habitual residence or domicile within the meaning of point (b) of Article 6(1) of Regulation (EC) No 593/2008, and point (c) of Article

17(1) of Regulation (EU) 1215/2012. In particular, where a trader acting, in accordance with Articles 3, 4 and 5 does not block or limit customers' access to his or her online interface, does not redirect customers to a version of his or her online interface that is different from the online interface to which the customer first sought access, regardless of their nationality or place of residence or place of establishment, does not apply different general conditions of access when selling goods or providing services in situations laid down in this Regulation or where the trader accepts payments instruments issued in another Member State on a non-discriminatory basis, that trader shall not be, on those grounds alone, considered as directing his or her activities to the Member State where the consumer has the habitual residence or domicile.'

The contrary position would be to consider the consequence of this (proposed) legislation to be that traders operating online, cross-border in the single market are required to consider the potentiality of being sued in the courts of the place where the consumer is domiciled a cost of doing business. The presumption would be that any trader selling online, cross-border within the internal market 'directs such [commercial or professional] activities to that Member State [of the consumer's domicile] or to several States including that Member State, and the contract falls within the scope of such activities.' (Regulation 1215/2012[2], Art.17(1)(c)) Moreover, if the trader wanted to bring proceedings against a consumer, the trader would be required to bring such proceedings only in the courts of the Member State in which the consumer is domiciled. However, this position would in this author's opinion impose an unfair burden on emergent, small and medium-sized business by unduly burdening them with operational costs.

The interlink may be strengthened by thinking in terms of alternative solutions, such as online dispute resolution mechanisms or assistance by European consumer centres.

1.4. Questions related to the collaborative economy

Question 1.4.1

Discussion on the collaborative economy in our country has focused on the booking of accommodation by tourists via collaborative platforms such as Airbnb.com:

'Undoubtedly, the application of the concept of a collaborative economy to accommodation presents an important challenge to the tourism industry. The expanding,

[2] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

mass conversion of residential property to tourist accommodation can also prove to be detrimental and has a number of implications.

That of unfair competition is naturally a primary concern given hospitality operators are subject to various rules and regulations. Compliance with the latter comes at a cost, not to mention the onus of administrative obligations.

Moreover, licensed hospitality businesses are bound to ensure the health and safety of their guests and staff, while safeguarding the statutory rights of consumers in general. They also need to comply with employment regulations and many businesses also constantly invest in the development and training of their personnel, thus contributing to an ongoing, and I add critical, process of enhancing their quality of service offered. Operators of unlicensed properties are not bound by any of these considerations.

We acknowledge that the increased offer of accommodation on a commercial basis through 'sharing economy' platforms may also lead to a rise in the undesirable black economy. A side effect of this can also be a decrease in regular employment and the creation of irregular activity, which would, in turn, incentivise the growth of precarious and undeclared employment.'

Edward Zammit Lewis, Minister for Tourism, in an article published in the Times of Malta entitled 'The collaborative economy', 7 February 2017, accessible here: https://www.timesofmalta.com/articles/view/20170207/opinion/The-collaborative-economy.638870

The Malta Tourism Authority ('MTA') receives complaints from unsatisfied consumers. These may lead to enforcement action, consisting of a fine or an enforcement notice; the latter notice is for regularisation or closure. The notice can be appealed. There's an appointed appeals boards made up of a lawyer (chair) and 2 other persons nominated by the Ministry for Tourism. If the enforcement notice is for closure, you can appeal it but you remain closed until the appeal board decision; if it is for regularisation, the order is suspended until the appeal is heard. *In extremis* MTA can take a person in breach of relevant regulations to court.

Question 1.4.2.

The Malta Hotels and Restaurants Association ('MHRA') have chased the MTA about the renting out of unlicensed properties. They claim this is an instance of unfair competition.

In Mr Mifsud's view, licencing is not a significant deterrent; moreover, in his view the markets are not really competing with each other.

'Tony Zahra, president of the Malta Hotels and Restaurants Association, said the MHRA had no problem with new "channels and trends" in holiday rentals, provided users are properly licensed and registered for VAT.

"If this does not happen, then it destroys the level playing field and gives non-regulated people an unfair advantage, since regulation carries costs," Mr Zahra said.

"Furthermore, regulated accommodation is inspected and classified, giving a level of comfort to consumers."

Mr Zahra added that the MHRA has been warning the Government about the proliferation of non-licensed accommodation for the past three years, saying this results in a substantial loss of revenue through fees and taxation for the State.'

[source: 'Unlicensed room letting risks penalty of €23,000: Property owners making a fast buck using website to attract tourists', Times of Malta, 13 October 2013, by Patrick Cooked, accessible here: https://www.timesofmalta.com/articles/view/20131013/local/Unlicensed-room-letting-risks-penalty-of-23-000.490062]

Question 1.4.3.

In Malta, if a person rents a property, or part of it, to a tourist, he or she must comply with existing Malta Tourism Authority ('MTA') regulations; in the first instance this requires an application for a licence.

The Malta Travel and Tourism Services Act (Cap.409 of the Laws of Malta) provides a definition of a 'tourist' in Art.2 as follows:

'"tourist" means any person who is travelling to and staying in places outside his usual environment for not more than one consecutive year for leisure, business and other personal purpose other than by taking up employment or to establish a business in the place visited;'

Mr David Mifsud, responsible for Quality Assurance & Licencing at the MTA, explained that the licences are there to ensure standards are upheld by those providing a service – in this case, by those persons involved in the accommodation sector. He said that the licence fees are not high and should not act as a hindrance to individuals from applying for a licence.

Mr Mifsud explained that there currently are two types of licences – one for host families, and the other for those renting out holiday furnished premises. So far, the host family licence is not only geared for those renting out a room/s to students, but also to ones renting a room/s to tourists.

[source: Malta–EU Steering & Action Committee (MEUSAC) Event 'Consultation Session: Collaborative Economy', 17 November 2016, accessible here http://meusac.gov.mt//eventdetails?ed=319]

The Malta Travel and Tourism Services Act, Art.18, states:

'(1) No person shall run or operate a hotel, guest house, hostel, holiday premises or catering establishment unless he shall have previously obtained and is in possession of a licence.

(2) No person shall provide accommodation in a house to tourists unless he shall have previously obtained and is in possession of a licence:

Provided that this subarticle shall not apply to the provision of such accommodation to bona fide relatives or friends when such accommodation is provided without any payment.

(3) It shall not be lawful for any person to give on lease to a tourist or to allow a tourist to occupy under any title, a house in Malta, or to transfer to any tourist any right of lease, or other title to occupation, of any such house, and for any tourist to take on lease or under any title to occupy a house in Malta, or to acquire any right of lease or other title to occupation of any such house, unless there is in respect of any such house a valid licence issued by the Authority authorising such lease, transfer or occupation.'

The definition of 'holiday premises' provided under the Malta Travel and Tourism Services Act is as follows: 'any building, howsoever described, but not being a hotel, guest house, hostel or the ordinary residence of the owner or tenant thereof, as the case may be, in which accommodation, ancillary services, including self-catering services, and amenities are provided for tourists; and includes any number of such buildings which are grouped together; and "keeper of holiday premises" shall be construed accordingly;'

Subsidiary Legislation 409.10 'Host Family Accommodation Regulations' defines a 'host family' as 'the person in whose name the licence for the accommodation of tourists has been issued and who resides in any building, howsoever described, not being a hotel, guest house, hostel or holiday premises, which is normally used for the permanent or temporary habitation of the licensee and is used or intended to be used for the concurrent habitation of guests;'

Subsidiary Legislation 409.11 'Holiday Premises Regulations' defines a 'holiday premises' as having 'the same meaning as assigned to it in the [the Malta Travel and Tourism Services Act] and shall include apartments, studios, villas, maisonettes, townhouses and terraced houses and other accommodation as the Authority may approve to fall within the said category.'

Mr Mifsud also noted that the Ministry for Tourism is in the process of revising legislation in relation to this sector. New legislation may provide separate licences for host families hosting students; and for those offering accommodation services via online platforms.

[source: Malta–EU Steering & Action Committee (MEUSAC) Event 'Consultation Session: Collaborative Economy', 17 November 2016, accessible at http://meusac.gov.mt//eventdetails?ed=319]

Mr Mifsud observed that, while the market is evolving, legislation is rather static; this is currently being addressed in the context of a revision of relevant

legislation ('Tourism Legislation Review' process). Current legislation will be amended to recognise new types of operations; for e.g. the host family licence will now be split into 2 separate licences: the host family licence will be exclusively for students (same as today); and a new 'bed and breakfast licence' will be introduced for those wishing to host tourists – in urban conservation areas it will be possible to host up to 16 persons; while in non urban conservation areas it will be possible to host up to 6 people (always space permitting).

In brief, Malta is out to regulate the collaborative economy:

From the draft proposed legal reform for the tourism industry, 'Standards, Criteria and Guidance Documents: Document A – Tourism Accommodation

> '3.3 Other Category of Accommodation
>
> When an innovative proposal for a tourism accommodation establishment does not qualify under any of the definitions provided in these regulations, the Authority may consider, in exceptional circumstances, awarding a basic license that is Unclassified, until a new category is established with appropriate criteria under which such tourism accommodation establishment shall be licensed. This type of Unclassified License shall be accompanied by any standards and conditions as may be determined by the Authority.'

The licencing/authorisation procedures for the licencing of certain types of accommodation issued by the MTA are simple, clear and transparent.

The Quality Charter, which came into effect on 1 June 2017, addresses the timeframes required to obtain a licence to operate a Holiday Furnished Premises (HFP) or a licence to operate as a Host Family. Through this Charter, MTA's Quality Assurance & Licensing Directorate, in collaboration with the authority's Enforcement Directorate, is committing itself to complete the required process within a period of 15 working days. This is subject to two conditions being met, namely:

1. that the application is submitted to the Authority together with all the required documentation, and
2. that when inspected, the relative property is found to be according to the standards as per legislative requirement.

[source: Quality Charters at http://www.mta.com.mt/quality-charters]

Question 1.4.4.

This author's research did not reveal any instance of actual legal challenges being brought, certainly not any being brought against any collaborative platform.

Mr Mifsud noted that all complaints made to the MTA are investigated and the absolute majority result in an on-site inspection to verify the complainant's version. Complaints about standards are all investigated.

Mr Mifsud explained that consumer issues are referred to the consumer affairs authority – the Malta Competition and Consumer Affairs Authority ('MCCAA'). MTA do try to resolve the issues but in matters of consumer protection and consumer rights, the appropriate thing to do is to direct the consumer to the consumer affairs authorities. The consumer affairs authority may ask MTA for a report. There is very good communication between the MTA and the MCCAA.

The author's contact at MCCAA contacted the European Consumer Centre ('ECC') Net Malta to enquire about these matters. The response received was the following: With regard to whether any complaints have been made to the ECC Malta in the context of peer-to-peer provision of services, ECC Malta informed that they do not have any registered complaints but that they did receive two (2) queries from Maltese consumers on problems they had regarding two (2) flats rented through *Airbnb*. In these cases ECC Malta advised consumers to write to the landlord, as they could not carry out the mediation since the transactions were between private individuals (C2C).

ECC Malta also reported having received another case more recently against *Airbnb*'s cancellation policy. The consumer cancelled the booking and the trader informed the consumer that the service fee of €182 had been retained. The consumer contested this sum on the fact that on the cancellation policy the following is stated:

> 'Cancellation Policy: Strict
>
> Cancel up to 30 days before your trip and get a full refund. Cancel within 30 days of the trip and get a 50% refund of the total nightly rate, as well as a full refund of fees.'

The case was subsequently shared with ECC Ireland against *AirBnb* on the basis of unfair contract terms. ECC Ireland requested the booking confirmation from the consumer but (as of 14 September 2017) the consumer has not yet come forward with this information. At the time of my latest communication with MCCAA/ECC Malta, the mediation had not yet taken place and ECC Malta did not yet know the position of their colleagues at ECC Ireland. Unless the consumer provides the information requested, the case will be closed.

Question 1.4.5.

Definition of "trader" for the purposes of The Consumer Affairs Act, Cap.378 of the Laws of Malta:

> '(i) any person, including any body corporate or incorporate who in relation to any transactions or other matters covered by this Act or regulations made thereunder is acting for purposes relating to his trade, business, craft or profession;

(ii) any public body, whether corporate or unincorporate, which provides goods or services to consumers for a fee;

(iii) any person to whom article 4 of the Commercial Code applies:

Provided that the Minister after consulting the Council may from time to time by Order published in the Gazette, designate as a "trader" for all or any purposes of this Act, any category or class of persons and any body corporate or incorporate whether established by law or not. Any Order made by the Minister as aforesaid may by like Order be amended, substituted or revoked;'

Commercial Code (Laws of Malta, Cap.13), Art.4 definition of 'trader':

'The term "trader" means any person who, by profession, exercises acts of trade in his own name, and includes any commercial partnership.'

Under Maltese law no minimum threshold is required to qualify as a trader. From the perspective of the MTA, if a person rents a room out once, one-off, for a fee, there is a licence requirement.

Question 1.4.6.
Legal rules which include balanced, reasonable standards within properties, accompanied by an efficient monitoring set-up, would definitely help in improving general consumer confidence.

Yes, Mr Mifsud believes in online ratings and reviews: when you have several complaints on the same operation, that is a sign!

Other appropriate tools could include: easy access to and familiarity with dispute resolution mechanisms.

2. Digital Media

Question 2.1.
The AVMS Directive was intended to cover TV broadcasting and on-demand services. It was not intended to include the website of a newspaper. This results clearly from the *traveau preparatoires* and other documented earlier reports.

In fact: cf. AVMS Directive recital (28) provides: 'The scope of this Directive should not cover electronic versions of newspapers and magazines.'

And cf. the Court of Justice in *New Media Online GmbH v Bundeskommunikationssenat* (case C-347/14) stated:

'recital 28 in the preamble to Directive 2010/13 cannot be understood as meaning that an audiovisual service must systematically be excluded from the scope of that directive solely on the ground that the operator of the website of which that service is part is a publishing company of an online newspaper. A video section which, solely

as part of a website, meets the conditions to be classified as an on-demand audiovisual media service, does not lose that classification merely because it is accessible on the website of a newspaper or because it is offered within that site.

An approach systematically excluding from the scope of the directive services managed by publishers of daily online newspapers due to their multimedia nature, without assessing on a case-by-case basis the 'principal purpose' of the service at issue, would not sufficiently take into account the diversity of the situations which could be envisaged and would run the risk that operators effectively providing audiovisual services within the meaning of Article 1(1)(a)(i) of that directive might be able to use a multimedia portal in order to evade the legislation which is applicable to them in that area.'

Prof Kevin Aquilina does not agree with the judgement. To the best of this author's knowledge, our national practice is not in line with this judgment. We follow the Directive as originally intended and as interpreted by the European regulatory authorities that meet at the European Platform of Regulatory Authorities ('EPRA').

The Broadcasting Act (Cap.350 of the Laws of Malta) Art.16G defines 'on--demand audiovisual media service' as 'a non-linear audiovisual media service provided by a media service provider for the viewing of programmes at the moment chosen by the user and at his individual request on the basis of a catalogue of programmes selected by the media service provider;' This is in fact a *verbatim* transposition of the text of the AVMS Directive.

A newspaper portal has no 'catalogue of programmes' and therefore it should not be covered.

The author was unable to confirm with the current CEO of the Broadcasting Authority, Dr Joanna Spiteri, that this position is indeed in line with current practice.

Question 2.2.

In Professor Aquilina's opinion, from a regulatory point of view it is a step in the right direction. Professor Aquilina believes that the extension of scope of application towards video-sharing platforms should go as far as the rules on protection of minors and the combatting of hate speech – as these raise concerns impinging upon human dignity and matters of societal harm; there is a public interest to ensure protection from this harm. However, regulating the commercial part makes no sense on the Internet.

Pierre Cassar also raised the matter of difficulty with implementation of the regulatory rules in practice, and questioned in particular which jurisdiction would be faced with regulation?

No, our national legislation does not already provide for sector-specific rules for audio-visual platforms.

Question 2.3.
As far as this author is aware, never. We follow the country of origin principle.

Question 2.4.
In Malta, the Broadcasting Authority ('BA') is a Constitutional body, enshrined in Articles 118 and 119 of the Constitution of Malta.

Relevant legal provisions:

> Art.118(2) provides: 'The members of the Broadcasting Authority shall be appointed by the President, acting in accordance with the advice of the Prime Minister given after he has consulted the Leader of the Opposition.'

On security of tenure, Art.118(5) provides: 'Subject to the provisions of this article, the office of a member of the Broadcasting Authority shall become vacant

(a) at the expiration of five years from the date of his appointment or at such earlier time as may be specified in the instrument by which he was appointed; or

(b) if any circumstances arise that, if he were not a member of the Authority, would cause him to be disqualified for appointment as such.'

And Art.118(6) provides: 'A member of the Broadcasting Authority may be removed from office by the President, acting in accordance with the advice of the Prime Minister, but he may be removed only for inability to discharge the functions of his office (whether arising from infirmity of mind or body or any other cause) or for misbehaviour.'

Art.118(8) provides: 'In the exercise of its functions under article 119 (1) of this Constitution the Broadcasting Authority shall not be subject to the direction or control of any other person or authority.'

Constitution Art.124 (10) provides: 'No provision of this Constitution that any person or authority, shall not be subject to the direction or control of any other person or authority in exercising any functions under this Constitution shall be construed as precluding a court from exercising jurisdiction in relation to any question whether that person or authority has performed those functions in accordance with this Constitution or any other law.'

Article 119 of the Constitution mandates that the Broadcasting Authority is to ensure due impartiality in broadcasting 'is preserved in respect of matters of political or industrial controversy or relating to current public policy and that broadcasting facilities and time are fairly apportioned between persons belonging to different political parties.'

Article 13(2) of the Broadcasting Act provides: 'In so far as general interest broadcasting services are concerned and where the Authority allows news and current affairs programmes to be broadcast by such services, it shall be the duty of the Authority to satisfy itself that, so far as possible, the programmes broadcast by any general interest broadcasting service complies with all or any of the following requirements as the Authority may impose in the broadcasting licence, that is to say – (...)

(f) that due impartiality is preserved in respect of matters of political or industrial controversy or relating to current public policy:

Provided that, except in the case of public broadcasting services, in applying paragraphs (c) to (f), the Authority shall be able to consider the general output of programmes provided by the various broadcasting licensees and contractors, together as a whole:

Provided further that the Authority may, when granting a broadcasting licence for a commercial station, impose any of the requirements mentioned in paragraphs (a) to (f) in the said licence.'

Article 13(4) of the Broadcasting Act provides: 'It shall also be the duty of the Authority to organise from time to time schemes of political broadcasts (including political spots) which fairly apportion facilities and time between the different political parties represented in Parliament; to produce properly balanced discussions or debates that afford access to persons from different interest-groups and with different points of view, and also to produce commentaries or other programmes about questions relating to current public policy, wherein persons taking part can put forward differing views and comments.'

The Hon. Dr. Francis Zammit Dimech commented that whether the Authority will in practice always act as an independent and autonomous body (or whether it has always acted like that) will ultimately depend on the integrity and good intentions of whoever occupies the post of Chairman, and that in turns depends on the extent to which government tries to really factor in the consultation with the opposition in that appointment, and in any case an effort is made to find a person who would rise to meet those obligations.

'It might be thought that because the Broadcasting Authority is established by the Constitution of Malta as an independent body, then government does not have any say in its functioning. This is however far from being the case. Government has over time controlled the Broadcasting Authority not in for as its decision making powers in terms of article 119 of the Constitution are concerned but in other ways.'[3]

[3] Aquilina, Kevin. 2013. The independence of the Maltese broadcasting regulatory authority: legend, wishful thinking or reality? Int. J. Public Law and Policy 3(2):141-156, at p.144.

'According to the Constitution of Malta, the Broadcasting Authority is appointed by the President of Malta on the advice of the Prime Minister after the latter has consulted the Leader of the Opposition. As a matter of practice this has worked out as follows since the late eighties/early nineties. The Prime Minister chooses two representatives; the Leader of the Opposition chooses another two; and the Prime Minister and the Leader of the Opposition consult with regard to the Chairman. If both agree on a suitable candidate, then s/he is appointed Chairman of the Authority; if no agreement is reached, then the Prime Minister may decide to tender his advise to the President of Malta and the latter has to make the appointment. Essentially the President has no say in the matter in terms of the Constitution and thus is bound to take the Prime Minister's advice. The President might have reservations as to the appointment of the Chairman and/or Members of the Authority. But if the Prime Minister decides to press ahead – as he is fully entitled to do so in terms of the Constitution – the President must comply with the Prime Minister's advice or, if he is adamant to do so, he is at full liberty to resign from office. The President's role is insignificant in the whole process. Not only so but the tendency is to choose members according to party lines and a Chairman who is considered to be acceptable to both main political parties represented in Parliament.'[4]

Constitutionally-speaking the Broadcasting Authority is independent, but in practice it is made up of two (2) members of the Labour Party ('Partit Laburista', or 'PL'), two (2) members of the Nationalist Party ('Partit Nazzjonalist' or 'PN'), and a Chairman effectively chosen by the government of the day. So its independence is doubtful, especially in cases where the smaller political parties need to go to the Authority which is made up of the larger parties – so where is the independence?

The Chairman may be removed from office in the same way he is appointed: by the President on the advice of the PM, on the same grounds as the judiciary (but in the case of the judiciary, the inability to discharge the functions of his office (...) or misbehaviour must be 'proved'; and also two-thirds majority of parliament is required[5]). As far as Prof Aquilina knows there has been no case of a

[4] Aquilina, Kevin. 2010. Updating Maltese Broadcasting Law to Present Day Realities in the Light of the Doctrines of the Rule of Law and of the Separation of Powers, accessible here http://www.statecareandmore.eu/index.php/35-blog-section/kevin-aquilinaas-category/157-updating-maltese-broadcasting-law-to-present-day-realities-in-the-light-of-the-doctrines-of-the-rule-of-law-and-of-the-separation-of-powers

[5] The Constitution of Malta Art. 97(2) 'A judge of the Superior Courts shall not be removed from his office except by the President upon an address by the House of Representatives supported by the votes of not less than two-thirds of all the members thereof and praying for such removal on the ground of proved inability to perform the functions of his office (whether arising from infirmity of body or mind or any other cause)or proved misbehaviour.'

Chairman being removed from office (although there have been cases of chairmen resigning because of clashes with the government of the day.)

In an article published in 2013, Professor Aquilina concludes that the Broadcasting Authority unfortunately does not satisfy the criterion of total independence from government and Parliament.[6] He carries out his analysis in the context of a five-fold taxonomy of independence, emerging from Council of Europe Recommendation Rec (2000)23 *on the independence and functions of regulatory authorities for the broadcasting sector*:

1. Independence as to the decision making and taking process;
2. Institutional independence (in so far as the appointment, composition, dismissal and functioning of the broadcasting regulator is concerned);
3. Financial independence;
4. Regulatory independence (in so far as regulatory powers, granting of licences and monitoring broadcasters' programme output are concerned);
5. Operational independence – in the sense of good governance (in so far as the regulator exercises its independence in an accountable, public and transparent fashion).

Classifying the BA as an 'independent regulator' (but not a 'totally independent regulator'), Aquilina states:

> 'This category fits perfectly well in the case of the Broadcasting Authority which has the final say in so far as decisions concerning constitutional broadcasting matters are concerned. The Constitution quite emphatically provides in article 118(8) that 'In the exercise of its functions under article 119(1) of this Constitution the Broadcasting Authority shall not be subject to the direction or control of any other person or authority.' Hence neither Parliament nor Cabinet may legislate or give directions to the authority in so far as its constitutional functions are concerned but may do so in so far as its legal functions under the Broadcasting Act (or any other ordinary law for that matter) are concerned. So in its prime function – the constitutional function – the authority enjoys full independence from the legislature and the executive. The authority's decision may, nonetheless, be challenged before a court of law. This is because article 124 (10) of the Constitution expressly provides that: 'No provision of this Constitution that any person or authority, shall not be subject to the direction or control of any other person or authority in exercising any functions under this Constitution shall be construed as precluding a court from exercising jurisdiction in relation to any question whether that person or authority has performed those func-

[6] Aquilina, Kevin. 2013. The independence of the Maltese broadcasting regulatory authority: legend, wishful thinking or reality? Int. J. Public Law and Policy 3(2):141-156.

> tions in accordance with this Constitution or any other law.' Hence, it is only the court and not the two other organs of the state which can review the Authority's workings but such review is not absolute: it is limited only to ascertaining whether or not the authority has acted within its powers, that is, intra vires its powers.'[7]

Professor Aquilina responded in the affirmative – that he would consider the introduction of such independence requirements for media regulators at EU level a step forward and that the EU should follow *Council of Europe Recommendation Rec (2000)23 on the independence and functions of regulatory authorities for the broadcasting sector.* He also does believe such development would facilitate the creation of a single market for audio-visual media services. The Hon. Dr. Francis Zammit Dimech expressed a similar opinion.

No, there are no national legal obstacles to such independence requirements for media regulators.

The Hon. Dr. Francis Zammit Dimech stated that in his opinion there have been various cases of undue political pressure. Nevertheless, much as there have been cases brought before the courts which were decided against the BA, in these cases the court ruled on the ground of incorrect exercise of discretion, not of undue political pressure as such.

There have been 2 cases regarding political pressure: there was one by Dom. Mintoff (of the Labour Party) against Montanaro Gauci, then Chairman of the BA,[8] which challenged decisions by the Broadcasting Authority as regards allocation of television airtime/a series of pre-election broadcasts where the BA had given the Progressive Constitutional Party as much airtime as the Labour Party and the Nationalist Party – and in fact the court had ruled in favour of the plaintiff, in favour of Mintoff; however, with reference to a specific allegation that Mintoff had made that there was some meeting by the Prime Minister of the day George Borg Olivier and the Chairman of the BA Montanaro Gauci, and that that would have led to some influence on the BA, the court rejected this allegation stating that the meeting was of a totally different nature and there was no indication of undue pressure.

Then there is the case of the Nationalist Party with regard to a broadcast that was going to be made by Mario Felice, spokesperson for finance. The broadcast had been recorded and part of the content of the broadcast was leaked to the Minister of Finance; there were contacts made by the Minister with the Chairman of the BA and the programme was withheld from being broadcast.[9] Stran-

[7] Op. cit. p.151-2.

[8] Dom. Mintoff vs Montanaro Gauci noe, First Hall Civil Court – 17/05/1971; Court of Appeal – 22/05/1971.

[9] [I have not yet managed to source the reference for this case.]

gely enough in this case the court ruled that this was not pressure, but merely the Minister 'alerting' the Chairman of the BA to check if there is anything that could lead to libel or defamation. FZD thinks it was a fine line.

Question 2.5.

Political advertising has been the most contentious.

The judgements delivered by the European Court of Human Rights (ECtHR)[10] and by the Maltese Courts[11] do not necessarily follow Maltese domestic law[12] on the subject of political advertising on the broadcasting media. On the contrary, they tend to be more critical of a total and straightforward broadcasting ban of political advertising and where they do admit such a restriction, they consider the immediacy and powerful effect of the broadcasting media at reaching more voters than other media do and that in certain well defined situations it is in the public interest to allow restrictions on the broadcasting of political advertising.[13]

In Malta, in its interpretation of an advertisement of a political nature, the Broadcasting Authority distinguishes between an announcement or a notice of a political event on the one hand, and an advert of a political nature on the other.

Whilst Maltese broadcasting law is written in a way to imply that it is imposing a wide-reaching broadcasting ban on political advertising, this is not the interpretation given by the Broadcasting Authority which distinguishes in its practice between an announcement and a political advert. The latter contains elements of propaganda or at least arguments trying to convince in favour of one particular view. This distinction is of relevance to political advertising as it allows announcements of political activities to be broadcast without any difficulty.

[10] *VgT Verein Gegen Tierfabriken v. Switzerland* [2001] ECHR 412, App No. 24699/94; *TV Vest AS & Rogaland Pensjonistparti v. Norway* [2007]ECHR, App. No. 21132/05. Cf. also *Murphy v Ireland*, Judgment on Merits, [2003] ECHR 352, App. No. 44179/98. More recently: Judgment on the merits delivered by the Grand Chamber *Animal Defenders International v the United Kingdom* [GC] [2013] ECHR 362, App No. 48876/08.

[11] General Workers Union v. Broadcasting Authority – Civil Court, First Hall, 3 June 2005; Constitutional Court 3 November 2006. Both national courts citing with approval with ECtHR's *VgT* judgement.

[12] Broadcasting Act (Cap.350) Article 13(4) 'It shall also be the duty of the Authority to organise from time to time schemes of political broadcasts (including political spots) which fairly apportion facilities and time between the different political parties represented in Parliament; to produce properly balanced discussions or debates that afford access to persons from different interest-groups and with different points of view, and also to produce commentaries or other programmes about questions relating to current public policy, wherein persons taking part can put forward differing views and comments.'; and Third Schedule, para 1: '1. Advertising and teleshopping shall not, except as authorized under a scheme of political broadcasts approved by the Authority in terms of article 13(4) of this Act, and irrespective of whether they are broadcast in return for payment or for similar consideration or otherwise, be of a political nature.'

[13] Aquilina, Kevin (2011) The freedom to impart political information vs. the absolute broadcasting ban on political advertising – a human rights perspective *Int. J. Private Law* 4(1):79-99.

> 'Whilst the European Court has moved on from an absolute ban of political advertising to a qualified ban, not all Council of Europe Member States have adopted that position in their laws. In the case study offered in this paper, the Maltese Courts have followed the European Court's case of *VgT* but the Maltese broadcasting regulator continues to follow the absolute ban on political advertising once Parliament has not amended the Broadcasting Act to bring it in line with the European Court and the Maltese Courts' judgements. This means that Malta – like some Council of Europe Member States which retain the absolute broadcasting ban on political advertising – is living in a dichotomy and is avoiding to square the circle. This can easily be done by Parliament opening a Pandora's box by enacting a law to amend the Broadcasting Act's provision on political advertising which is no longer tenable as there might be cases – like the General Workers Union case – where an absolute broadcasting ban on political advertising is in breach of the European Convention on Human Rights' and the Constitution of Malta's provisions on freedom of expression.'[14]

Note however that the article by Prof Aquilina pre-dates the case *Animal Defenders International v the United Kingdom*.[15] In *Animal Defenders* a majority of the Grand Chamber of the ECtHR held that the UK's statutory broadcasting ban on political advertisements under the Communications Act 2003 did not breach the right to freedom of expression under Article 10 of the ECHR. The judgment departs from the Court's previously established case law.

As a result, and in view of this judgement from the ECtHR, national case-law in Malta may need revisiting if a challenge is brought once again before our courts.

There were other contentious cases concerning hate speech. They are documented in the BA annual reports 2004 and 2008.[16] These cases concerned a certain Mr Norman Lowell and charges of incitement to racial hatred in terms of Article 13(2)(a) of the Broadcasting Act, read in conjunction with Article 82A of the Criminal Code which prohibits racial hatred. The various charges brought – including a judgement delivered by the Court of Magistrates (Malta) on 27 March 2008 finding Mr Norman Lowell guilty of incitement to racial hatred (and sentencing him to a two year prison sentence suspended for four years and a fine of EUR 500),[17] and confirmed by the Court of Criminal Appeal,[18] are dis-

[14] Aquilina (2011), at p. 96.

[15] *Animal Defenders International v the United Kingdom* [GC] [2013] ECHR 362, App No. 48876/08.

[16] Broadcasting Authority, Annual Report 2004, Hamrun, Broadcasting Authority, 2005, p. 18 and pp.53–55; Broadcasting Authority, Annual Report 2008, Hamrun, Broadcasting Authority, 2009, p.12.

[17] The Police v. Normal Lowell, Court of Magistrates (Malta), per Magistrate Dr Consuelo-Pilar Scerri Herrera, 27 Mar. 2008.

[18] Court of Criminal Appeal, inferior competence, per Mr Justice Lawrence Quintano, 15 Jul. 2013.

cussed in: Aquilina, Kevin. 2014. *Supplement 13 of the International Encyclopaedia of Laws/Media Law* – Case Law Related to Racial Hatred, p.147-150.

Question 2.6.
(Is this a reference to broadcasting on the Internet?)

Nothing new under national Broadcasting and/or data protection laws surely.

Question 2.7.
The author has not yet been able to identify any source of information on this matter from a national perspective.

Question 2.8.
The author has not yet been able to identify any source of information on this matter from a national perspective.

This author considers that the country of residence of the consumer does need to be controlled by the service provider on a regular basis, for commercial considerations; the conciliation of such requirement with the data minimisation principle under the GDPR could be achieved by ensuring the deletion of such data as soon as the purpose for which it has been collected has been achieved, as well as other (legal and technical) safeguards to ensure respect of the purpose/use-limitation principle.

3. Digital infrastructures

Question 3.1.
This response was provided by the MCA:

No, Malta did not have any rules in place on net neutrality.

MCA follows the approach suggested in the BEREC guidelines whereby each possible zero rating case is analysed on its own merits. Through the various activities undertaken since the coming into force of net neutrality provisions, the MCA did not identify any zero-rating or other traffic/price discrimination practices/offers on the Maltese market which are outright in breach of the Regulation. The MCA is, however, assessing whether IAS providers offering access to their IPTV platform, on a free-of-charge basis to their own mobile subscribers, constitutes a breach of the Regulation in line with the BEREC guidelines.

Question 3.2.
This response was provided by the MCA:

Telecommunications networks and services are regulated via a set of EU Directives, Regulations and Decisions which form part of what is known as the Electronic Communications Framework. Given the fast pace in the technologi-

cal and business models development, this framework is revised every few years in order to update the rules. Each time such a review is carried out, the EU institutions debate what needs to be done so that we have a truly single market. These debates would focus on market failures and barriers to entry, and would finally establish what the rules should be and the institutional lines over which tasks are more efficiently and effectively implementable, whether at EU level or national/local level. Some aspects may need to be enforced at an EU level while others are best left to national authorities to deal with given that they have the knowhow of the local market and relevant stakeholders.

In September 2016, the European Commission published a set of proposals with the intention to revamp the current set of rules. The proposals contain a number of recommendations that in the case of the notification process to start operating in the market (to start an electronic communications operation one does not need a license but only needs to notify the national regulator) and for spectrum-licensing are tantamount to EU-wide licensing schemes. While at face value these seem to be decreasing bureaucracy, in reality these would be shifting local enforcement powers up to the Commission. The Commission's Impact Assessment did not prove that there exist market failures or that the current rules create any barriers to entry or that implementation should be at an EU level. Therefore while a single market for telecommunications networks and services is very important, having for example EU-wide licensing schemes do not necessarily benefit the single market but might as well run counter to this same objective.

Malta boasts 100% coverage of broadband services. So, all Maltese households are able to get access to fixed broadband services at speeds of at least 30Mbps to 250Mbps nationwide. Speeds of 500Mbps are also offered in selected places. Investment if high-speed broadband networks is fully private funded and mainly driven by competition.

The overall number of subscriptions keep increasing year-on-year, particularly for products offering higher download speeds. Recent DESI figures indicate that Malta ranks 9th among EU countries in terms of take-up and well above the EU average. Underlying the considerable jump in take-up of superfast fixed broadband is the continued drive by service providers to upgrade existing customers to higher-speed products.

Malta has undertaken a number of demand driven initiatives such as the MCA Free Wi-fi project which aims to making Malta one of the first WiFi states in Europe and campaigns that promote the use of the smart phone as a productivity tool. Moreover, the MCA is implementing a number of measures to stimulate demand and increase take-up of broadband services. This includes helping people to have the skills and awareness about how the internet can be used, for

example, to achieve a better quality of life, through to personalised information eGov portals, e-commerce and internet banking and facilities for health and social care. In addition, the MCA has a number of initiatives with a particular focus on small and medium sized enterprises (SMEs) to support economic growth. This includes the promotion of cloud computing as a business innovator, mentoring, training and advice specifically targeted at the use of digitally-enabled technologies, and other focused activities to support business growth, especially amongst SMEs. All these initiatives form part of a wider strategy that the MCA is currently coordinating aimed at addressing the digital divide.

No broadband measure was the result of EU intervention.

Question 3.3.

This response was provided by the MCA:

There are no legal issues on spectrum management in Malta.

Question 3.4.

This response was provided by the MCA:

No, the independence of the MCA was never questioned. The independence of the NRA is enshrined in the EU Regulatory Framework Directive which is transposed under national law. Having said this, a few years back, following the transposition of a revised Framework, the European Commission had asked Malta to amend parts of the national legislation, including the provisions relating to the independence of the MCA, in order to make them clearer. Legislation was amended accordingly.

[end of response by the MCA.]

> 'Not all regulators are on the same footing in so far as their degree of independence from government is concerned. There are some who are more independent than others. For instance, there is no comparison between the constitutionally established Broadcasting Authority and the ordinary law established Malta Communications Authority or Mineral Resources Authority. Independence from governmental control thus varies from one regulator to another.'[19]

Professor Aquilina classifies the Malta Communications Authority as a 'low level of independence regulator':

> 'A low level of independence regulator is one which has some independent decision making powers but most of its decisions have to be endorsed by the government

[19] Aquilina, Kevin. 2013. The independence of the Maltese broadcasting regulatory authority: legend, wishful thinking or reality? Int. J. Public Law and Policy 3(2):141-156; at p.151.

or by Parliament. Such is the case of the Malta Communications Authority and the Mineral Resources Authority. In both cases the sword of Damocles hangs over each authority's head in terms of article 6 of the enactment establishing such authorities.'[20]

In so far as the Malta Communications Authority is concerned, Article 6 of the Malta Communications Authority Act (Cap.418 of the laws of Malta) reads as follows:

'6. (1) The Minister may in relation to matters that appear to him to affect the public interest, from time to time give to the Authority directions in writing of a general character, not inconsistent with the provisions of this Act, on the policy to be followed in the carrying out of the functions vested in the Authority by or under this Act, and the Authority shall, as soon as may be, give effect to all such directions:

Provided that the Authority shall act independently and shall not seek or take instructions from any other body on matters related to ex-ante market regulation and the resolution of disputes between undertakings in accordance with articles 43 and 44A.

(2) The Authority shall afford to the Minister facilities for obtaining information with respect to its property and activities and furnish him with returns, accounts and other information with respect thereto, and afford to him facilities for the verification of information furnished, in such manner and at such times as he may reasonably require.

(3) If the Authority fails to comply with any directions issued under this article, the Prime Minister may make an order transferring to the Minister in whole or in part any of the functions of the Authority.'

Professor Aquilina is of the view that, until the law is amended, whatever government or the MCA state, the position remains that the MCA is totally and completely at the mercy of government. He therefore disagrees with the view of the chairman of the MCA for the provision in question mentions no extraordinary circumstances when the power in that provision is to be exercised or not. The solution is to have that provision repealed.

4. Data in the digital economy

Question 4.1.

A core strategy group was set up consisting of representatives from: the Ministry for Social Dialogue, Consumer Affairs and Civil Liberties, the Office of the Attorney General, the Ministry for Home Affairs and National Security, and the Office of the Information and Data Protection Commissioner ('IDPCO'). The

[20] Op. cit. at p.152.

group is tasked to look at the GDPR (Regulation 2016/679) and the Directive on data protection in the police and criminal justice sector (Directive 2016/680). Eventually, when the discussion taking place will be about the ePrivacy Directive/(proposed) Regulation, the Malta Communications Authority (MCA) will also form part of this group. The core strategy group is undertaking a provision by provision review of the GDPR to discuss the impact on national legislation and national practice and draft the amendments to the current law. Our national Data Protection Act will be amended so as to repeal any provisions that would overlap/conflict with the new Regulation and leave or introduce new provisions implementing those Articles of the Regulation that allow some discretion to the Member State at national level in terms of: specifications, options, limitations and regulatory duties. The process is being led by government (not by the IDPCO). The IDPCO follows the advice of the Office of the AG in terms of legal drafting.

Question 4.2.
The IDPCO provides guidance and support to businesses in line with their mission statement and their obligations under data protection law. The Office also performs its duties in the context of prior consultation exercises to provide advice to controllers as per obligations under the national Data Protection Act/forthcoming GDPR.

Question 4.3.
So far, to the best of the author's knowledge, such contentious issues have not arisen.

Question 4.4.
Yes, the IDPCO has received some requests from data subjects to have search results deleted (delisting) from the Google search engine. The IDPCO facilitates the process by providing guidance to data subjects on how to exercise their legal rights. In the first instance the request may be made directly by the data subject to Google through the dedicated link provided by the search engine itself on its portal. If Google does not accede to the request, the data subject may lodge their complaint with the IDPCO. As Google does not have any legal presence/establishment and therefore no controller in Malta, the IDPCO lacks jurisdiction. The IDPCO in Malta will either guide the data subject to lodge the complaint with the Irish DPA (where Google have their European headquarters); alternatively, complaints lodged with the IDPCO are forwarded to the Irish DPA for them to investigate. Under the GDPR, in such situations the 'consistency mechanism' would then kick in and the Maltese IDPCO would be a 'concerned' DPA.

NORWAY

Torger Kielland*
Stian Øby Johansen*
Hilde K. Ellingsen*

Introduction

This report is written as a coherent text, and we have found it neither possible nor prudent to answer all of the questions posed in the questionnaire. Some are simply not relevant under the Norwegian system, whilst others have not been the subject of great concern to Norwegian courts or policy makers. We have therefore chosen to focus on a few selected issues that we hope will prove beneficial to the comparative aims of the FIDE-project.

From the outset, it is important to stress that since Norway is not a member of the EU, but rather a party to the EEA Agreement, our national report will deviate somewhat from the reports from the EU member states. The particularities of the EEA Agreement are explained in the national report on taxation, state aid and distortions of competition, and will therefore be left out in the following.

1. Internal market and electronic commerce: Internet and e-commerce

1.1. Electronic Commerce, liability of Internet intermediaries

Most of the Norwegian cases regarding intermediary service providers concerned the intermediaries' liability for providing services for sites giving access to copyright infringing material.

In 2009, several rightholders sought a preliminary injunction against one of Norway's major telecommunication providers – Telenor – to compel the company to block access to *thepiratebay.se*, *piratebay.net*, *piratebay.org* and similar domain

* University of Bergen and University of Oslo.

names. The Court of Appeal concluded that Telenor could not be held liable for contributory infringement to the sharing of copyrighted material that was facilitated by Pirate Bay.[1] Therefore, there were no grounds to issue a preliminary injunction.

In 2013, the Copyright Act was amended. Under the new Section 56c, the Court may order telecommunication service providers «to prevent or impede access to a site where material that obviously violates copyright or other rights under this Act is made available on a large scale». For a motion to be granted the arguments in favour of granting the order must outweigh the drawbacks the order will entail. In this respect, the Court shall weigh the arguments in favour of granting the motion against the interests affected by such an order, including whether the order is directed at the owner of the website, and the consideration of freedom of information and expression. One should also take into consideration the possibility of less restrictive measures.

Following the introduction of Section 56c, the rightholders filed a new motion to restrict access to Pirate Bay and similar sites in accordance with the new rules. The District Court found that Pirate Bay and the other sites violated copyright on a large scale, and that the interests of the rightholders outweighed the interests of the telecommunications providers and the owner of the website. The Court therefore ordered Telenor and other telecommunications providers to DNS block thepiratebay.se, piratebay.net, piratebay.org and similar domain names and prevent them from being accessed by their customers.[2] The rightholders also requested that the Court establish a procedure to prevent so called «domain name shuffle», where a site changes its domain name to a new one once the old one is blocked. This was rejected by the Court, as the Copyright Act required a new order for additional domains to be added to the list of blocked domains.[3]

In sum, the general rules on preliminary injunctions did not provide for an order to block access to Pirate Bay and similar sites, and a change of law was therefore required. Yet the effect of DNS blocking and denying end users access to copyrighted material that is made available on the Internet without authorisation is debatable. If there is any measurable effect it is probably more of a signal to users that unauthorised copying is not tolerated.

Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

The most contentious issue concerning remedies under the Consumer Sales and Guarantees Directive in Norway is probably to what extent a consumer can

[1] LB-2010-6542 (Borgarting Court of Appeal 2010).

[2] Order of Oslo District Court of 1.9.2015, TOSLO-2015-67093.

[3] Additional sites were later added to the blocking list by way of a new decision, TOSLO-2016-72899.

demand a replacement of a faulty good or has to settle for a repair. A case concerning a broken heel of a woman's boot went all the way to the Supreme Court (!). Replacement of the boot would cost approximately €55, while repair would cost around €8. The case hinged on whether the cost of replacement was disproportionate to the cost of the repair, cf. Article 2 no. 3 of the Directive. Ultimately the Supreme Court found that the Directive was not decisive. A majority of three judges found that the consumer could not demand a replacement and had to settle for a repair. A minority of two judges found that the consumer could demand a replacement.

Both the proposed Directive on certain aspects concerning contracts for the supply of digital content (COM(2015)634), and the amended proposal for a Directive on certain aspects concerning contracts for the online and other distance sales of good (COM(2017) 637 final), aim for a maximum harmonization of the rules regulated in those Directives, cf. Article 5 and Article 3.

In light of the aim to establish a digital single market, such maximum harmonization seems to be the only sensible path. Given this overall aim to facilitate online shopping and the provision of digital services in the single market, anything but a maximum harmonization would function as a restriction on this market. For consumers such harmonization is, as a rule, an unconditional advantage, as it safeguards the same level of protection with regard to online purchases and digital services across Europe.

Such maximum harmonization, however, implies that some countries will have to provide a lower level of consumer protection than they currently do. The Norwegian authorities seem to be particularly concerned about the proposal to limit the time period during which a consumer is entitled to a remedy to two years (COM(2017) 637 final Article 14). Under the Norwegian Consumer Sale of Goods Act, the relevant time period is set to be five years for goods that are intended to last substantially longer than two years.

There is a legitimate concern that shorter time limits for remedies may lead to a reduction in product quality. Given the cross-border element of online purchases, however, maximum harmonization appears to be crucial to promote a digital single market. Even if the Norwegian authorities seem to be prepared to argue for a lower level of harmonization, this seems unlikely to succeed in terms of time limits for remedies, since all EU Member States – except Sweden, Finland and the Netherlands – have already limited the length of time within which the consumer can claim a remedy.

Thus far, there have been no actions before Norwegian courts on the basis of consumer law against online providers' terms and conditions. In 2006, however, the Norwegian Consumer Ombudsman initiated a case against Apple claiming that some of iTunes Store's terms and conditions were unfair and therefore con-

trary to the Norwegian Marketing Control Act. In particular, the condition that music bought on the iTunes Store could only be played on Apple's iPod and the DRM that restricted playback on other devices.

The case was brought before the Norwegian Market Council – an administrative «court of law» that, among other things, carries out supervision of the Marketing Control Act. Yet, the case was settled before the Council had an opportunity to consider the case. Apple agreed to alter the DRM of the files offered on iTunes to allow them to be played on other media players than Apple's iPods.

1.3. Geo-blocking

Article 4 of the proposed Regulation on ensuring the cross-border portability of online content services (COM(2015) 627 final) lays down the rule that the provision of an online content service, including access to and use of such a service, shall be deemed to occur solely in the subscriber's Member State of residence. This is so even when the subscriber accesses the service while travelling abroad to another Member State. This is self-evident if one is to achieve any kind of portability of online services that the Regulation aims for. Yet the scope of the proposed Regulation is limited to subscribers who are *temporarily* present in another Member State. If this condition is fulfilled, it is evident that the Regulation's «member state residency»-rule should apply.

There could, however, arise borderline cases. In Central Europe, an online service originating in one Member State could easily be used by residents living in another Member State, even if their presence there is not temporary, but rather permanent. Citizens domiciled in one Member State could also subscribe to online services in another Member State (for example because the service is cheaper or gives access to different content). My impression from speaking with Norwegian rightholders is that such cross border use will not be a big problem in Norway. Yet, one must still consider to what extent such use lays outside the proposed Regulation and will be regulated by the general rules of jurisdiction in the Brussels II Regulation, or to what extent that use is excluded from the scope of the Regulation.

2. Digital media

The Audiovisual Media Services Directive (AVMS Directive) was transposed into Norwegian law in 2012, essentially by amendments to the Norwegian Broadcasting Act (the Act relating to broadcasting and audiovisual on-demand services). The Norwegian Media Authority (hereafter NMA), is the regulatory authority in charge of supervising compliance with the provisions of the Act. The NMA is independent both legally and factually. According to the Norwegian Broadcasting Act Section 2-15, the Ministry cannot instruct the NMA in individual cases.

Moreover, when preparing the annual public broadcasting report, the NMA cannot take instructions from the Government or the Ministry, cf. Section 2-13 of the Broadcasting Act. Decisions of the NMA are, pursuant to the Broadcasting Act Section 2-14, handled by the independent Media Appeals Board.

The scope of the Broadcasting Act is determined with due regard to the AVMS Directive. In *New Media Online* (Case C-347/14), the European Court of Justice construed the concept of 'programme' of Article 1(1)(b) of the AVMS Directive broadly, so as to include the provision of videos of short duration consisting of local news bulletins, sports and entertainment clips, by an online newspaper, provided that the principal purpose test is met. There is a wide variety on online newspapers in Norway, and most of them offer audiovisual content. The Norwegian Media Authority is well aware of the ECJs judgment, and interprets the Broadcasting Act in conformity with the Court's findings.

Since the AVMS Directive is a minimum harmonization directive, Norway has opted for stricter and more detailed rules on issues of general public interest. In line with Article 4(1) of the Directive, Norway has used the opportunity to ensure a higher level of protection in areas such as health, gambling and the protection of minors. Children are protected against harmful programmes (cf. Act on Protection of Minors from Harmful Audiovisual Programmes); advertising specifically directed at children is prohibited (Section 3-1 Broadcasting Act, cf. Marketing Act Section 19-21); advertising for alcoholic beverages is prohibited (Section 9-2 Alcohol Act), and the amount of advertising is severely restricted (Section 3-1 Broadcasting Act). The effectiveness of these stricter Norwegian rules is undermined, however, by the borderless nature of online audiovisual content.

The country-of-origin principle has given rise to challenges in Norway. Audiovisual media service providers can provide their services in the EU/EEA by complying only with the rules of the host country. Hence, Norway cannot prevent the reception of media services from providers established in other EU/EEA countries, provided they comply with the rules of the AVMS Directive. There are media service providers established in jurisdictions with less strict regulations targeting a Norwegian audience, thereby avoiding the stricter regulatory framework in place. Such targeted broadcasts often expose the Norwegian audience to unwanted content.

One of the most contentious issues has been the marketing of gambling services. Norway has opted for a high level of consumer protection in the area of gambling. To offer gambling services, a license issued by the Norwegian authorities is required, and operators without such a license are prohibited from advertising their services. Yet, due to the country-of-origin principle, Norwegian viewers are exposed to gambling commercials stemming from international gambling oper-

ators targeting the Norwegian market. Norwegian citizens are thereby encouraged to avail themselves of online gaming services not subject to Norwegian jurisdiction. Commercials sent from broadcasters established in other EU/EEA countries thereby undermine the effectiveness of the legislative framework in the gambling sector.

The "consultation procedure" contained in Article 4(2) has not proved able to remedy the situation, given that the sending country can only encourage, and not ban, such broadcasts. Moreover, the possibility of adopting "appropriate measures" in instances where a broadcaster attempts to circumvent the stricter rules in a specific EU/EEA state, cf. AVMSD art. 4(3), is narrow. The regulatory authority must prove that the service provider has established himself in another country to circumvent the specific rules in question, and proving such intent is not an easy task.

Broadcasters exclusively targeting a Norwegian audience is nothing new, and it has been perceived as a problem for decades. This can be illustrated by the ruling of the EFTA-Court in *Lego/Mattel* (Joined Cases E-8/94 and E-9/94), concerning the interpretation of Directive 89/552/EEC ("Television without frontiers"). The Norwegian Market Council asked the EFTA Court for an advisory opinion in two cases brought before it by the Consumer Ombudsman against Mattel and Lego, respectively, for alleged infringements of the Norwegian ban on television advertising directed towards children. Lego and Mattel had broadcasted commercials on TV3, which broadcasted from the United Kingdom via satellite television.

The EFTA-Court stated that the responsibility for regulating the activities of broadcasters and ensuring compliance with the relevant legal framework mainly rests with the transmitting state, and the receiving state must mainly refrain from restricting retransmission on their territory of broadcasts emanating in other Member States. The Court made clear that advertising directed specifically at the receiving state is also within the scope of the Directive. The Court held that the rules of the Directive covered also the behavior of advertisers (see, however, Joined Cases C-34-36/95, *de Agostini*, where the ECJ reached the opposite conclusion).

3. Digital infrastructures

Norway has a long running regulatory regime on net neutrality. Before the adoption of Regulation (EU) 2015/120, Norway had no legally binding rules on net neutrality. Yet, we had a set of national guidelines drawn up by the Norwegian Communications Authority (hereafter NCA) in collaboration with stakeholders in the industry, such as the Internet Service Providers, industry organisations, content providers and consumer protection agencies. These guidelines did not have

any formal legal status, but were rather a soft law instrument prescribing 'best practices'. However, although the NCA was not able to sanction infringements, the authority monitored the internet service providers and encouraged compliance. Due to wide endorsement by the industry, the guidelines worked as intended.

The guidelines set out three overarching principles for the handling of data traffic by internet service providers: First, Internet users were entitled to an Internet connection with a predefined capacity and quality. Second, internet users were entitled to an Internet connection that enabled them to send and receive content of their choice; use services and run applications of their choice and connect hardware and use software of their choice that did not harm the network. Third, Internet users were entitled to an Internet connection that was free of discrimination with regard to the type of application, service or content or based on sender or receiver address. The principles, which were of a rather broad and general nature, were further expanded on in the guidelines.

The national guidelines on net neutrality were replaced by legally binding provisions in March 2017. Regulation (EU) 2015/120 was transposed into Norwegian law through amendments in the Electronic Communications Act and the Electronic Communications Regulation. Although the national guidelines have been phased out, the NCA benefits from years of experience with matters pertaining to net neutrality.

The European rules on net neutrality bear similarities to the previous Norwegian guidelines, given that both sets of rules deal with transparency, reasonable traffic management and the opportunity to offer specialized services in parallel with the Internet access service. Having said that, the Regulation seems to be less strict when it comes to zero-rating. Under the old regime, the NCA considered that zero-rating would constitute a violation of the net neutrality guidelines. Consequently, Norwegian operators did not adhere to a practice of zero-rating at the time. This is different under the Regulation, which provide the regulators with powers to intervene based on a comprehensive assessment covering several criteria, as specified in BERECs Guidelines on the Implementation by National Regulatory Authorities (NRAs) of European Network Neutrality Rules.

The NCA is still sceptic towards zero-rating. Yet, the authority now conducts a case-by-case assessment, applying Regulation (EU) 2015/120 and BERECs Guidelines. Norwegian internet service providers have launched various offers in the market such as music streaming services and internet radio. Thus far, the NRA has handled three cases, one of which ended without any decision on the merits, another still pending and a third allowing the practices to continue for the time being.

The NCA is an autonomous agency of the Ministry of Transport and Communications. The agency is self-financed, primarily through fees and charges.

Geographically, the agency is located far away from the industry stakeholders, as its head office is in Lillesand. The Ministry of Transport and Communications decides on appeals against decisions made by the NCA and can in certain instances overturn its decisions. The Ministry may not instruct the NCA, either generally or in specific cases (cf. Section 10-2(2) Electronic Communications Act). Yet, the Ministry may instruct the authority to consider cases within the scope of the Electronic Communications Act (cf. Section 10-2 of the Act).

The regulatory regime in the telecom sector was subject to debate in the late 1990s. The Ministry of Transport and Communication was at the time the owner of the telecommunications operator Telenor. It was also the appeals body for decisions taken by the NCA in individual cases, as well as vested with certain regulatory functions. The EFTAs Surveillance Authority (ESA) issued a reasoned opinion to Norway, stating that the regulatory regime in place at the time was not in compliance with the independence requirement set out in the Telecommunications Services Directive (90/288/EEC) and the ONP Framework Directive (90/387/EEC), as amended by Directive 97/51/EC. To ensure a structural separation between ownership functions and regulatory functions, the ownership of Telenor was transferred to the Ministry of Trade and Industry.

4. Data in the digital economy

Norway is an EEA country with a dualistic legal system. Consequently, the direct application of the General Data Protection Regulation (GDPR) in Norwegian law is contingent on the completion of two additional steps: *First*, the GDPR must become part of the EEA agreement. This requires a unanimous decision of the EEA Joint Committee, which as of December 2017 has yet to be made. When the Joint Committee Decision enters into force, probably before 25 May 2018, the GDPR will become binding on Norway as a matter of EEA/international law. *Second*, since Norway has a dualist legal system, the General Data Protection Regulation (GDPR) must be transposed in order for it to become binding on individuals. The Government has therefore drafted legislation that makes the regulation part of Norwegian law. A public consultation on the draft law took place from June to October 2017. The Government will put its final legislative proposal before the Storting (parliament) in the spring semester, with the aim of having the law enter into force simultaneously with the entry into force of the GDPR on 25 May 2018.

The entry into force of the GDPR will also require a myriad of amendments to more specialized laws and regulations. For examples, public consultation is underway on the draft proposals to amend the Immigration Act and the Immigration Regulation. The different Government departments are also undertaking studies to identify other legislative and regulatory measures that need to be taken before the entry into force of the GDPR.

There seems to be a fair amount of awareness about the GDPR among Norwegian businesses – at least about the basic facts that it will enter into force in 2018 and that it does entail significant changes in the law. Part of the reason for such awareness might be the abundance of courses held by law firms and other experts on the impact of the GDPR.

The Norwegian law on such matters as the "Internet of Things", autonomous vehicles and systems, *et cetera* is still at an embryonic stage. The law usually lags behind the technological development, making this area of law resemble a game of catch-up. With regard to some matters, EU regulations is the only source of innovations. For example, in late 2015 the Law on Intelligent Transport Systems (ITS) was enacted, in order to have a legal basis for implementing EU Commission regulations in the area. So far, Regulations (EU) 885/2013, 886/2013, and 962/2015 have been implemented through the ITS law.

Examples of more autonomous Norwegian developments do exist in some areas, however. For instance, in December 2017 the Storting (parliament) approved a new law on the testing of autonomous motor vehicles. Under this law, one can apply for a permit to test autonomous vehicles. The permits given may, on a case-by-case basis, exempt the autonomous motor vehicle in question from requirements under the Norwegian Road Traffic Act and the Professional Transport Act.

Moreover, the use of drones for commercial and recreational purposes has sparked some debate in Norwegian mass media over the last few years. In 2015 the Government therefore enacted a regulation on "aerial vehicles without a driver on board", which regulates all forms of drone use in Norway – from model airplanes to large commercial drones. In order to promote compliance among hobbyists, the Norwegian Civil Aviation Authority has established an online website with easy (and visual) explanations of the rules at www.dronelek.no.

The CJEU's controversial May 2014 judgment in the *Google Spain (Costeja)* case has had a measured impact in Norway. The brunt of de-listing requests from Norwegian individuals appear to have been submitted directly to the search engines themselves. Google's Transparency Report shows that just over 16 000 URLs have been removed from their search index following complaints from Norwegians (an approval rate of approximately 50 %). In contrast, only 85 Norwegians have filed "right to be forgotten"-complaints with the Norwegian Data Protection Authority (Datatilsynet) per September 2017. The Data Protection Authority estimates that it rejected about half of these complains.

Individuals that are not satisfied with decisions of the Data Protection Authority have a right of appeal to the Data Privacy Appels Board (Personvernnemnda). Only two cases concerning the "right to be forgotten" appear to have been decided on the merits.

The first case, no 17/2014, concerned a request by an individual that the publisher "Schibsted" should delete a number of old articles in the (online) newspapers it publishes. The complaining individual referred to the then recently decided *Google Spain* case. However, in its decision the Data Privacy Appeals Board did not discuss *Google Spain* at all. It merely stated that the articles had a journalistic purpose, and thus were covered by the right of freedom of speech.

The second case, no 10/2016, directly concerned a de-listing request against Google. The individual in question sought to remove search results pointing to an online forum thread identifying him as having been convicted for crimes, including rape and pedophilia. It was undisputed that the allegations were true. Google rejected his de-listing request, but the Data Protection Authority concluded that Google should de-list. Google then complained to the Data Privacy Appeals Board. In its decision, the Board interpreted the Norwegian Personal Data Act in light of the *Google Spain* judgment, and found that the criteria established by the CJEU had to be applied to decide the matter. It also referred to the guidelines of the Article 29 Data Protection Working Party. The Board then engaged in an extensive assessment *pro et contra*, ultimately concluding that Google should remove the disputed search index entry.

POLAND

Dr hab. Jakub Kociubiński*

Explanatory note: Author made a conscious effort to focus (whenever is possible) exclusively on the acquis of Polish doctrine highlighting issues described in this report. Given country-specificity of this report, quoted sources should not be treated as a reference for the presented issues in general but as an as broad as possible representation of works of Polish researchers. Since most quoted sources, especially acts of domestic law, do not have an official English version, all translations in the text are author's unless stated otherwise. Although Polish scholars and other sources are quoted extensively providing a valuable reference, all conclusions, assessments and especially expressed viewpoints in this report are solely author's. Other opinions (mostly institutions') are always presented with explicit reference to their sources. The author takes credit for any possible errors. This report presents the state of the law as of May 24th, 2017.

1. Internal Market and electronic commerce : Internet and e-commerce
1.1. Electronic Commerce, liability of Internet intermediaries

Question 1.1.1.

Definition of Intermediary Service Provider – ISP [pol. *pośredniczący dostawcy usług*] can be described and defined through a certain number of sub-concepts existing in Polish legal order[1]: The services, broadly speaking, delivered elec-

* PhD, LLM. Associate Professor at the Chair of International and European Law, Faculty of Law, Administration and Economics, University of Wrocław, Poland. [jakub.kociubinski@uwr.edu.pl].

[1] M.Z. Zieliński, *Odpowiedzialność deliktowa pośredniczących dostawców usług internetowych. Analiza prawnoporównawcza*, LEX Wolters Kluwer Business 2013, pp. 41-42. Note: The abbreviation ISP could denote both Intermediary Service Providers as well as Internet Service Providers. Former meaning will be used throughout this report.

tronically, defined in Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market as "information society services" [pol. *usługa społeczeństwa informacyjnego*] while in Polish Act on the Provision of Electronic Services which implements mentioned directive these services are described as "service provided electronically" [pol. *usługa świadczona drogą elektorniczną*][2]. Additionally, it's worth to mention that in a case law of Polish courts the term "electronic service" [pol. *usługa elektroniczna*] while not being strictly speaking legal is often used[3].

The definition of "information society services" initially provided in Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC (replaced by Directive 2015/1535/EU which uses the same wording)[4] has been expanded by Polish lawmakers so its equivalent "service provided electronically" is described as: "every service provided without simultaneous presence of parties (on distance), on individual recipient's request by data transfer sent and received through devices for electronic processing including data compression, and storage of data transmitted through telecommunication networks in the meaning of Act of July 16th 2004 Telecommunication Law"[5]. Despite the semantic difference in core terms, it is widely accepted in the doctrine that "information society services" and "service provided electronically" are synonymous[6].

A significant difference between the literal wording of Directive 2000/31/EC and Polish implementing act lies with an understanding of the key concept of "service provider" [pol. *usługodawca*]. In the latter act, this notion is limited to persons acting "at least incidentally" [pol. *chociażby ubocznie*] in their professional

[2] Act on the Provision of Electronic Services [*Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną*], Dz.U. 2002 nr 144 poz. 1204 ze zm. The Act predates Poland's membership in the EU and had been enacted as a part of State's adaptation to the EU's *acquis*.

[3] Especially in case-law of Polish courts. See *inter alia* judgment of District Court in Wrocław [pol. *Sąd Okręgowy we Wrocławiu*] 23.07.2010, I C 144/10; of the Court of Appeal [pol. *Sąd Apelacyjny*], 15.01.2010, I Aca 1202/09. See also P. Sadowski, *Udostępnienie utworu w Internecie ze szczególnym uwzględnieniem udostępnienia na stronie WWW*, Przegląd Prawa Handlowego (3)2009, pp. 47-52.

[4] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 Laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, OJ L 204, 21.7.1998, p. 37; Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, OJ L 217, 5.8.1998, p. 18–26. Act has been replaced with the Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 17.9.2015, p. 1–15.

[5] Article 3(4) Act on the Provision of Electronic Services. See also J. Gołaczyński, *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Wolters Kluwer 2009. Telecommunication Law [*Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne*, Dz.U. 2004 nr 171 poz. 1800, ze zm.]. „Telecommunication network" [pol. *sieć telekomunikacyjna*] is defined in Article 2(35).

[6] X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Difin S.A 2004, s. 65.

capacity and/or for profit[7]. This approach runs contrary to well-established *acquis* of EU law where even incidental one-time service provision falls under the definition of economic activity even if it is not for profit[8].

It could be argued (and it seems there is a consensus in the doctrine) that the term "service provider" should be interpreted broadly to reflect *telos* of Directive 2000/31/EC despite clear inconsistency between it and the Polish Act on the Provision of Electronic Services. As a result, there is a considerable number of rather confusing attempts to interpret as to what kind of activity have professional or for-profit character[9]. Especially it is not entirely clear whether persons involved in "hobbyist" activities in the web like running a fan page, forum, and so forth will be outside the scope of Act on the Provision of Electronic Services[10]. If not, it is true they will not be burdened by some requirements stipulated by the Act, but at the same time, they wouldn't be able to invoke special rules for liability (especially derogation of liability for activities of third parties uploading potentially illegal data on these websitesWhile controversial, it fits into the general definition of an entrepreneur and economic activity in Civil Law according to which an activity must be carried out by a professional entity in an organised and professional manner. See further analysis in Questions 1.4.4 and 1.4.5.

[7] M.Z. Zieliński, *Odpowiedzialność deliktowa pośredniczących…*, p. 45. It is worth to mention that the definition presented above have an autonomous character and should be treated as *lex specialis* of generic notion. There are significant differences in wording with other, general definition provided in: Article 43^1 of the Civil Code [*Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny*, Dz.U. 1964 nr 16 poz. 93, ze zm.) which is considered to be a general, normative definition. Additionally the notion of "entrepreneur" (pol. p*rzedsiębiorca*, which is used in similar manner as the term "undertaking" in EU law) which covers service providers is provided in Article 4 of the Act of Freedom of Economic Activity [*Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej*, Dz.U. 2004 nr 173 poz. 1807, Consolidated Version Dz. U. z 2016 r. poz. 1829, 1948, 1997, 2255]; in Article 2 of the Act on Combating Unfair Competition [*Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji*, Dz.U. 1993 nr 47 poz. 211, ze zm.] in Article 2(1) of the Act on Counteracting Unfair Market Practices [*Ustawa z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym*, Dz.U. 2007 nr 171 poz. 1206 ze zm.].

[8] See details in J. Kociubiński, *Usługi swiadczone w ogólnym interesie gospodarczym w prawie Unii Europejskiej*, TNOiK, 2013 including quoted literature and case-law.

[9] In case-law of Polish courts is often emphasized that economic activity, including provision of services, should be carried out in a "continuous and organized manner" [pol. *w sposób ciągły i zorganizowany*]. See *inter alia* Supreme Court's judgment [pol. *Sąd Najwyższy*], 22.10.2003, II CK 161/02, OSN 2004, nr 11, poz. 186;
16.05.2006, I UK 289/05, OSN 2007, nr 11-12, poz. 168; 12.09.2006, I UK 106/06, OSN 2007, nr 17-18, poz. 260 and judgments of the Voivodship Administrative Court in Gliwice [pol. *Wojewódzki Sąd Administracyjny*] in cases: 13.11.2013 I SA/Gl 152/15; 08.10.2015, I SA/Gl 152/15, and of Voivodship Administrative Court in Gdańsk 09.03.2010, I SA/Gd 17/10. List is by no means exhaustive.

[10] In the light of above interpretation if a person have a full-time occupation and as a side activity is operating "hobbyist" website would under "service provider" definition especially when the website contains advertisement banners and/or donation possibility. Even if a person have no other occupation these mentioned functionalities of a given website would determine status of its operator as a "service provider".

Moreover, some doubts persist whether service provider (in the meaning presented above) could at the same time be an owner of the servers where data uploaded by the customers are being stored. It is something which is not directly regulated by the Act on the Provision of Electronic Services, although it is widely accepted that "resellers" are also covered by the regulation[11]. The term "reseller", which have no direct and non-descriptive translation in Polish, refers to undertakings facilitating online trade (both B2B and B2C) by providing retailers with for example dedicated software or servers[12]. The practical problem is that data could potentially be stored in practically every place in the world not necessary in the company's headquarters' country[13]. Additionally, storage services are routinely outsourced, so one could argue that service provider could at the same time be a recipient of service. This potential overlap of legal situations of provider and recipient has not been explicitly recognised in the Act on the Provision of Electronic Services[14]. Article 2(7) provided only minimalistic guidance by defining "service recipient" [pol. *usługobiorca*] as "any natural person, legal entity, an organisational unit without legal personality who uses the service provided electronically". It may be argued that implementation not be precise enough to this point, but at the same time, a teleological and pro-EU interpretation with reference to the original wording of Directive 2000/31/EC seems sufficient[15].

Further distinctive issue with the delimitation of the notion of ISP's scope arise pertaining to establishing provider's liability. Up until 2008 Polish Act on the Provision of Electronic Services contained serious lacunae as, contrary to Directive 200/31/EC, liability exemption could've only applied to ISPs providing data transfer, not access to data[16].

[11] The term is not strictly speaking legal, as neither Directive 2000/31/EC nor Polish law uses it. Here is used in general understanding of the word to denote situation when an entity is at the same time a "service provider" and "recipient of service" under abovementioned acts.

[12] The word „reseller" do not exist in the Polish Language Dictionary (PWN, 2017) but has been adopted into common language in its original English form. The closest Polish translation would be "*pośrednik sprzedaży*" which literally translated as "sales intermediary".

[13] M.Z. Zieliński, *Odpowiedzialność deliktowa pośredniczących...*, p. 48. This was the case of eBay's entry into Polish market where servers that stored data of Polish customers were stored abroad.

[14] During preparatory work that finally leads to adoption of the Act on the Provision of Electronic Services an alternative translation of Directive 2000/31/EC has been published. It expanded the definition of "service provider" by adding following phrase at the end: "or shares them" [pol. *lub jej udostępniania*]. Such addition would more than likely completely solve mentioned overlap problem, yet it has not been introduced into legal text. See D. Kot, *Dyrektywa Unii Europejskiej o handlu elektronicznym – tłumaczenie*, Kwartalnik Prawa Publicznego (1)2001, p. 176.

[15] X. Konarski, *Komentarz do ustawy...*, p. 77.

[16] The Act has been amended in 2008 by *Ustawa z dnia 7 listopada 2008 r. o zmianie ustawy o świadczeniu usług drogą elektroniczną* (Dz.U. 2008 nr 216 poz. 1371).

The problem with the legislation regulating ISPs engaged in hosting comes up in relation to liability exemption as stipulated in the Article 14(1) of the Act on the Provision of Electronic Services. Analysis of the wording of this provision shows some significant difference with the relevant provision of Directive 2000/31/EC. Hosting service providers – sub-category of ISPs are in much more favourable position under Polish law than it stems from the literal wording of Directive 2000/31/EC[17]. The national provision does not distinguish between the various legal basis of liability[18]. It is however not necessarily contrary to Directive 2000/31/EC as it could be argued that it provides only minimal standard and States be free to increase the level of legal protection as they see fit[19]. Yet it remain doubtful as the Directive 2000/31/EC clearly indicates aim to harmonise rules for intermediaries' liability[20]. Therefore, it seems these rules do not constitute a minimal but the standard intended by EU lawmaker. Any results contrary with this standard indicates an incorrect transposition[21]. Additionally, it is highly doubtful whether these differences in wording between Directive and Polish act could be ameliorated through either pro-European interpretation of the national law or by direct application of mentioned directive[22]. Furthermore, provision described above could be problematic considering CJEU's ruling in *L'Oréal v eBay* case as discussed in question 1.1.2.

Question 1.1.2.

In author's opinion, the approach of the CJEU's ruling seems to be overzealous. The main problem lies with the notion of "active role" of the intermediary service provider[23]. One can reasonably argue that every online service allowing uploading product's photos (with for example some basic editing like for instance

[17] M.Z. Zieliński, *Odpowiedzialność deliktowa pośredniczących...*, p. 195.

[18] W. Chomiczewski, *Wybrane problemy odpowiedzialności host providera w internecie według prawa polskiego*, Biuletyn Prawno-Podatkowy 1(3)2008, p. 50.

[19] See D. Kot, *Dyrektywa Unii* Europejskiej..., p. 89; A. Matlak, *Prawo autorskie w społeczeństwie informacyjnym*, Wolters Kluwer Polska SA 2004, p. 171; P. Podrecki, Z. Okoń, P. Litwiński, M. Świerczyński, T. Targosz, M. Smycz, D. Kasprzycki, *Prawo internetu...*, p. 213; G. Rączka, *Ochrona usługobiorcy usług elektronicznych*, TNOiK 2007, p. 291.

[20] See Recital 40 of the Preamble of the Directive 2000/31/EC.

[21] W. Chomiczewski, *Wybrane problemy odpowiedzialności...*, p. 50.

[22] Requirement of pro-European interpretation of national provisions is well established and widely accepted in case-law of Polish court although should be limited that it would not produce *contra legem* results – against literal wording of domestic provision (See judgments of the Supreme Court, 19.10.2012, III SK 3/12; 13.12.2012, III SK 23/12; of the Supreme Administrative Court [pol. *Naczelny Sąd Administracyjny*], 20.03.2012, I FSK 847/11; 12.09.2012, I FSK 1781/2011). Direct application of Directive 2000/31/EC is not possible because it would amount to imposing obligations on individuals.

[23] "Active Role" is defined in § 112-116 of the judgment C-324/09 *L'Oréal SA and Others v eBay International AG and Others* (ECLI:EU:C:2011:474). The Court to a large extent repeated its reasoning from earlier joined cases C-236/08 to C-238/08 *Google France SARL and Google Inc. v Louis Vuitton Malletier SA, Google*

cropping), adding product's description will fall under "active role" under CJEU's definition[24]. It effectively means that practically all online trade platforms –service providers – as per Electronic Commerce Directive 2000/31 parlance, could be held liable for not exercising sufficient control over hosted traders.

While it might be argued that in principle the intermediary service provider should not be totally exempted from liability for goods being traded on administered platform. The rigorous approach taken in CJEU's *L'Oréal v eBay* ruling causes some practical problems: In the CJEU's line of reasoning liability is absolute, provided "active role" can be established. However it is highly arguable whether providing "(...) assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting them (...)" is a conscious process by the operator (during which it can gain knowledge that the goods in question are illicit), or is it a rather an automatic process utilizing in-built website's functionalities[25].

It, therefore, remains questionable whether the intermediary service provider will always be able to establish if third party products that are being offered, are indeed counterfeit. Which brings up the question as to what kind of mechanisms could be utilised here, as mentioned providers lack any formal investigative powers so the efficiency of any of their checks is at best debatable. Subsequently, these could become fictitious given that regardless of how thorough provider's assessment will be its liability could not be ruled out. In any case, this could drive up the costs especially for the end-users (buyers) as trade platforms will look for means to offset the costs of product-checking.

To sum it up, the most obvious merit of the liability test in question is that it is straightforward in use. However, the price of its interpretative simplicity is the arbitrariness. Therefore, author is of the opinion that *L'Oréal v eBay* interpretation is overly stringent and inflexible effectively devoiding Article 14 of the Directive 2000/31EC of its purpose.

Question 1.1.3.

Attempt to introduce a dedicated notice-and-takedown rule into Polish legal order provides an instructive case study of its advantages and drawbacks[26]. In 2011

France SARL v Viaticum SA and Luteciel SARL and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (ECLI:EU:C:2010:159) § 114-120.

[24] According to this line of reasoning one could speculate that everything apart from providing information about price and product name excluding manufacturer's name would fall under "active role". It stands to reason that it makes absolutely no business sense to operate such bare-bones trading platform.

[25] See para 123 of the Judgment, where Court assessed that such assistance falls under „active role".

[26] The concept of notice-and-takedown comes from US Digital Millennium Copyright Act, Pub. L. 105-304. Throughout this analysis the notion will be used with the reference to its original version.

Ministry of Internal Affairs and Administration published a proposal of amendment the Act on the Provision of Electronic Services which seeks to introduce the notice-and-takedown mechanism[27]. According to the proposal, a person who becomes aware of illegal content could sent notification [pol. *powiadomienie*] to the service provider[28]. Within three working days provider could either block this content or refuse it. In the former case person responsible for this content could appeal to service provider within three working days. The provider could then accept or reject this appeal – lift the blockade or keep the content in question blocked[29].

The principal problem with this proposal is its complete arbitrariness. Acceptance or refusal of blockade request, and at later stages lifting blockade was purely discretionary. Lawmakers failed to provide even minimum guidance to assess "trustworthiness" of notices. The notice-and-takedown principle originally came from US Digital Millennium Copyright Act (DMCA), but attempt to implement it on Polish ground had been at best half-hearted. In its original form the procedure is protected by sanction – disregarding notices excludes the possibility to invoke liability exemption clause encapsulated in US equivalent of Article 14 of the Directive 2000/31/EC. In US liability exemption does not apply to anonymous entities (there is registration requirement). Additionally, under DMCA person abusing takedown request by providing false claims could be held liable[30]. Polish lawmakers envisaged none of these safeguards.

Furthermore, according to Article 15(1) of the Directive, 2000/31/EC Member States shall not impose a general obligation on electronic services providers, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. The introduction of notice-and-takedown in proposed form would result in the necessity of constant monitoring of published content by site administrators. Therefore it runs contrary to Directive's *ratio legis* and most likely with the proportionality principle[31].

[27] Proposal Draft Proposal for a Bill Amending Act on the Provision of Electronic Services (Submitted to Committee on European Affairs) [*Projekt założeń do projektu ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną (skierowany do rozpatrzenia przez Komitet ds. Europejskich)*] was published on 26.01.2011 in Public Information Bulletin [pol. *Biuletyn Informacji Publicznej* – BIP]). Text is available at https://bip.mswia.gov.pl/bip/projekty-aktow-prawnyc/2011/19323,dok.html (01.04.2017).

[28] *Projekt założeń do...*, p. 29.

[29] Ibidem.

[30] See C. Wolf, *The Digital Millennium Copyright Act: Text, History, and Caselaw*, Pike & Fisher, Silver Spring MD 2003.

[31] It is doubtful whether these additional obligations imposed on site administrators are indispensable for achieving goals, and these goals could not be reached by other, less restrictive means. In any case, every regulation that is not within objectives of a given directive will "automatically" fails proportionality test.

To conclude, in author's opinion the principle behind notice-and-takedown mechanism is sound. The problem with Polish attempt to introduce this concept comes from the fact that project completely omitted safeguards. The whole system was completely arbitrary and thus prone to abuses. Proposed regulation could've either be used as a powerful tool for censorship or could've been completely disregarded. It is hard to predict which route could've been taken but both were equally plausible under proposed rules. At the same time the very need for a mechanism that could help to remove illegal content i.e. libellous, slandering, infringing IP is necessary. It is therefore quite puzzling that Polish lawmakers failed to substantiate the need for proposed regulation[32]. Advocate General Jaaskinen in opinion in case *L'Oréal v eBay* even claimed that principle of notice-and-takedown is already enshrined in Directive 2000/31/EC[33]. The original incarnation of this rule in DMCA is arguably more stringent than European regulations, but the dedicated notice-and-takedown mechanism would only work if there are sufficient safeguards against abuses in place. Something that Polish lawmakers completely neglected. Ultimately the proposal has not been adopted and currently, in Polish law, there is no dedicated notice-and-takedown rule.

Nevertheless, under current rules possibility to bring offline offending content is possible in principle. Polish lawmaker quite faithfully transposed Article 14 and 15 of the Directive 2000/31/EC into domestic legal order. These provisions are seting up a liability regime for (broadly speaking) hosting services allowing a waiver if a service provider with due diligence was not aware of the offending nature of the content[34]. *A contrario* should a service provider be informed (with reasonable probability) about allegedly offending content; the entity could be held liable for its continuous hosting[35]. It provides a very rudimentary notice-and-takedown mechanism, but the problem with its practical application lies

See further A. Frąckowiak-Adamska, *Zasada proporcjonalności, jako gwarancja swobód rynku wewnętrznego Wspólnoty Europejskiej*, Wolters Kluwer 2009.

[32] It is truly bizarre that in discussed project under header "The Need and Purpose of Adopting the Proposed Amendment" [*Potrzeba i cele uchwalenia projektowanej zmiany ustawy*] it is stated that "individual" [pol. *pojedyńcze*] judgments of Polish courts indicated that lack of specific regulation for exemption of website administrators' liability is problematic (p. 4). Maybe is just a poor choice of words, but stating that "individual" judgments are enough to introduce burdensome regulation is hard to explain.

[33] § 163 of the Opinion (ECLI:EU:C:2010:757).

[34] These are Articles 14 and 15 of the Act on the Provision of Electronic Services.

[35] Attempts of one of prominent ex-politician to block allegedly offending comments under online version of press articles and force publisher's apology and compensation serves as an instructive case study. The plaintiff claimed that Article 14 of the Act on the Provision of Electronic Services (equivalent of Article 14 of the Directive 2000/31/EC) should not disproportionally encroach on the right of a good name, and such intrusion in itself is unconstitutional. The plaintiff further claimed that Article 14 is incorrectly interpreted by the Polish court because, according to him, it should only apply to B2B relations. The indictment did not succeeded.

in the vagueness of its criteria. In reality, there is a certain "grey zone" where it was difficult to establish if a service provider was or should have been aware of the nature of hosted content.

Question 1.1.4.

In Poland, there've been some cases when national courts were considering injunctions [pol. *sądowy nakaz blokowania stron*][36]. These could be regarded as *quasi*-precedential as courts had minimal previous experience in dealing with this matter.

Attempt to block a popular allegedly "pirate" website by the group of IP holders serves as an instructive case study[37]. After nearly four years of court proceedings, in a case against individuals who uploaded questionable content, plaintiffs claiming that continuous operation of allegedly "pirate" website is causing significant losses to their IPs made an attempt to block its content until case resolution[38]. District Court in Warsaw refused, claiming that internet providers – intermediaries – are not parties to this case (neither participants in a legal sense) and therefore there can be no obligations imposed on them through Court order[39]. The District Court cited Article 755(1) of the Code of Civil Procedure which stated: "Court may regulate the rights an obligation of parties or participants in proceedings"[40]. The ruling brought up a serious question of whether injunctions are possible at all under Polish law.

At the same time, there are no doubts that injunctions are possible under EU law – point that was repeatedly restated in CJEU case-law[41]. Therefore the lack

[36] „Injunction" which in Polish is translated in descriptive manner as "Court's blocking order", or "Court's order to block websites" is not strictly legal term. In Polish law injunction measures falls under wider category of "Security of Claim" [pol. *zabezpieczenie rozczeń*] regulated in Article 730[1]§1 of the Code of Civil Procedure [pol. *Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego*, Dz.U. 1964 nr 43 poz. 296 ze zm.

[37] The defendant was accused of infringing Article 79(1)1 of the Copyright Law [pol. *Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych*], Duo. 1994 no 24 post. 83ze zm., also in relations with Article 422 of the Civil Code and of Article 18 of the Act on Combating Unfair Competition. Defendant requested to remain anonymous.

[38] Case XX GC 1004/12. Additionally there may be a data protection issue. Although in principle everybody can refuse to have its personal data published (with the exemptions provided by law) in the context of notice-and-takedown Data Protection Ombudsman [pol. *Rzecznik Ochrony Danych Osobowych*] stated in decision DOLiS/DEC-437/13 (18.04.2013) that request do bring down content containing personal data do not necessarily means that the content in itself is illegal.

[39] Similar reasoning in Court of Appeal in Kraków judgment 14.02.2013, I ACz 66/13, Court of Appeal in Warsaw judgment, 17.05.2013, VI ACz 922/13.

[40] J. Jankowski (ed.), *Kodeks postępowania cywilnego. Tom II. Komentarz Art. 730-1217. wyd 2*, C.H. Beck 2015, p. 104-108.

[41] See especially Cases C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH* (ECLI:EU:C:2014:192); C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH* (ECLI:EU:C:2009:107).

of an efficient mechanism of blocking offending content could be perceived as a possibly incorrect transposition of European regulations. It is true that currently, inductions are not possible during a proceeding against persons uploading illegal contents without any knowledge of its content[42]. However, plaintiffs could, in theory, start a separate proceeding against intermediaries (service providers) to obtain Court order. It is still problematic as it remains unclear what could be the subject of such case.

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.

By introducing Directive 1999/44/EC into Polish legal order lawmakers, in essence, created a separate legal regime for liability claims. Apart from the generic regime of contractual liability encapsulated in Article 471 of the Civil Code amendment that led to the adoption of Consumer Law changed (among others) Articles 566 and 574 of the Civil Code introduced a specific liability regime for physical and legal defects of goods respectively[43]. This distinction is especially problematic when given goods are being purchased for dual use – individual and business. In a result certainty of law suffers[44].

Nevertheless, it is widely accepted that specific sellers' liability regime for physical defects of goods provided by Article 566(1) of the Civil Code (and Article 574(1) for legal flaws) do not exclude separate compensatory claims under generic rules as per Article 471 of the Civil Code[45]. This issue remains controversial for some time but in mentioned amendment to the Civil Code legislator explicitly stated that these two legal regimes are not mutually exclusive[46]. However, the problem partially remains as there is a certain overlap between these regimes[47]. Generic one applies if sold goods turned out to be faulty while specific is

[42] See judgment of the Court of Appeal in Lublin, 18.01.2011, I ACa 544/10 where Court held that service providers are not required to monitor content published on the administered websites, and only when provider had prior knowledge (*implicite* from some other sources) about illegality of a given content then this service provider could be held liable.

[43] A. Kidyba (ed.), *Kodeks Cywilny Tom III, Zobowiązania*, LEX, Wolters Kluwer business 2014, p. 161 and 184-185.

[44] D. Karczewska, M. Namysłowska, T. Skoczny (eds.), *Ustawa o prawach konsumenta*, C.H. Beck 2015, p. 18.

[45] Non-exclusive nature of these two mechanisms is recognised in the case-law of Polish courts. Especially buyer who exhausted claims under generic rules governing warranty under Article 471 of the Civil Code retains right to claim compensation under Article 566 (or Article 574) of the Civil Code.

[46] M. Kaliński, *Szkoda na mieniu i jej naprawienie*, Warszawa 2011, p. 339.

[47] R. Strugała, *Odpowiedzialność odszkodowawcza sprzedawcy związana z realizacją uprawnień z tytułu rękojmi a ogólne zasady kontraktowej odpowiedzialności odszkodowawczej*, Transformacje Prawa Prywatnego (4)2016, p. 106.

applicable if the customer was not informed about a defect in the merchandise[48]. Although some interpretative controversies remain, it can be assumed that latter regime is limited to so-called "negative contractual interest" [pol. *ujemny interes umowny*][49]. Generic rules encapsulated in Article 471 of the Civil Code remain applicable to claims pertaining to "positive contractual interest" [pol. *pozytywny interes umowny*][50]. For remedies be granted under Article 566(1) (and analogously under Article 574(1)) of the Civil Code the customer must according to generic rules governing burden of proof prove that goods are defective, that warranty option had been exhausted [pol. *rękojmia*], and the existence of harm[51].

Additionally, it can be mentioned that the very notion of "Non-conformity of the Product with the Contract of Sales" [pol. *towar niezgodny z umową*] is ambiguous under Polish law. The complete legal definition of this concept is nowhere to be found although its meaning can be implicitly decoded from the implementing act[52]. Additionally, the notion can be constructed, or at least estimated, with reference to the Preamble of the directive 1999/44/EC which proves to be problematic in terms of legal certainty. It is often pointed in the doctrine that there is a *quasi*-presumption of conformity that can be rebutted but the question of burden of proof as well as of evidence standard remains[53].

Question 1.2.2.

Currently, in Polish legal order contracts for the supply of digital content do not have its own *lex specialis*. However, it is clear that under freedom of contracts principle as enshrined in Article 353 of the Civil Code contracts which have as its subject supply of digital content are allowed[54]. What remains controversial is the applicability of specific legal regime to these contracts (see also comments on question 1.2.1.)[55]. It largely stems from fact that digital content could possibly be distributed through various means – online, on hard drives – which creates certain ambiguity[56].

[48] Ibidem.

[49] See W. Czachórski: *Uwagi na temat pojęcia tzw. ujemnego interesu umowy*, Studia Cywilistyczne (XIII –X iV)1969, p. 14; M. Kaliński, *Szkoda na mieniu...*, p. 337.

[50] R. Strugała, *Odpowiedzialność odszkodowawcza sprzedawcy...*, pp. 101 et seq.; M. Kaliński, *Szkoda na mieniu...*, p. 343.

[51] A. Kidyba (ed.), *Kodeks Cywilny...*, pp. 164; M. Manowska, *Rękojmia i gwarancja*, Prawo Spółek (10)1997, p. 34.

[52] See further: E. Habryn-Chojnacka, *Niezgodność towaru konsumpcyjnego z umową sprzedaży*, Wolters Kluwer 2010.

[53] M. Koszowski, *Domniemanie czy definicja zgodności towaru z umową*, Ius Novum (2)2012, pp. 86-96.

[54] See *inter alia* P. Machnikowski, *Swoboda umów według art. 353(1) KC. Konstrukcja prawna*, C.H. Beck 2005.

[55] T. Targosz, M. Wyrwiński, *Dostarczanie treści cyfrowych a umowa sprzedaży*, Forum Prawnicze (1)2015, pp. 18–31.

[56] J. Pisuliński, *Stosowanie wspólnych europejskich przepisów o sprzedaży do treści cyfrowych* in: A. Matlak, S. Stanisławska-Kloc (eds.), *Spory o własność intelektualną. Księga jubileuszowa dedykowana profesorom Januszowi Barcie i Ryszardowi Markiewiczowi*, LEX Wolters Kluwer business 2013, pp. 799 and 815.

In this light the general aim of proposed directive should be approved. However, some salient points could be problematic, and could hinder achievement of a genuine digital market (the comments below applies to draft version as available on 28.03.2017):

The notion encapsulated in Article 2 of the directive proposal (points b and c) defines "digital content" [pol. *treści cyfrowe*] through the concept of "service" [pol. *usługa*]. It seems prudent to add word "supply" to "digital content" to create *sui generis* category because otherwise, the directive is treating the provision of digital content as a part of generic services.

Proposed directive introduces the concept of "digital product" [pol. *produkt cyfrowy*] without defining it. Therefore it is not clear what is the relation between this term and the notion of "digital content" [pol. *treść cyfrowa*].

It is unclear why in Article 3(2) of the Polish version of a draft the term "Customer" (pol. *klient*) has been used instead of "Consumer" [pol. *konsument*]. It has to be noted that in English version word "Consumer" is used. These terms – *klient* (customer) and *konsument* (consumer) – are not synonymous in a legal sense[57].

Additionally, there are some doubts as to what is the relation between paragraphs 1 and 2 of Article 3 of a draft directive. It is not clear whether "consumer's specifications" [pol. *wskazówki klienta*] in Article 3(2) refers to creative inputs relating to the content or just the decision on pre-prepared elements customer is choosing from (i.e.,. various Internet packages)[58]. In latter case where the customer is being given a choice of off-the-shelf products, it is difficult to argue that there is any influence on the actual "specification". "Specifications" could then only refers to the delivery method not the content in itself. On the other hand in reality customers hardly ever provides authoritative guide on the actual content. So one could argue that if digital content is being delivered without any recourse to "consumer's specifications" (although of course with customer's consent) such contract will be outside the scope of the proposed directive.

Article 8 of the directive proposal states that digital content "(...) shall be free of any right of a third party, including based on intellectual property (...)". Normative value of such wording is not clear instead the provision should contain clear-cut obligation to supply content free of any right of a third party[59].

[57] See analysis of the notion of consumer [pol. *konsument*] in question 1.4.4.

[58] Polish translation is problematic here. Word *wskazówki* used in Polish version translates into English as „guidance", „tips" „directions" rather than „specifications" (which would be translated as *specyfikacja*) as it is in the English text of the draft. Specifications would suggest more heavy involvement in creating service including inputs on its technical characteristics etc. while guidance would indicate just formulation of general outline. Regardless, both terms are ambiguous in a legal sense, although might open different interpretative possibilities.

[59] B. Lanckoroński, K. Kuszel, *Opinia na temat...*, pp. 125-126.

Finally, remedies envisaged in Article 12 of a new directive presents different regulatory model than currently existing in Civil Code especially after 2014 amendment and adoption of Consumer Law[60]. Directive provides for a sequential nature of possible remedies (described in Polish legal doctrine as "cascading nature " [pol. *charakter kaskadowy*])[61]. Conversely, Polish legislator is departing from this model towards a more streamlined linear solution, so mechanism envisaged in Article 12 of the draft directive seems to be a step back.

To sum up, it must be emphasised that controversies mentioned above and unclear areas not have major character relating to the very model and *ratio legis* of proposed directive. Proposed directive is a step in a right direction, although its quality regarding legislative technique leaves room for further improvement.

Question 1.2.3.

Looking at the question from Polish perspective, it is clear that there are some issues with the implementation of current European regulations (see especially section 1.4). Having said that full harmonisation could be problematic due to its deep intrusion into civil law[62]. It could lead to a lack of harmony between local legal traditions and "external" (European) rules[63]. Of course, it stands to reason that preserving national traditions should not be a goal in itself, especially when these domestic regulations offer a lower standard of individual protection. Therefore, the key issue is how seamlessly European regulations can be introduced into national legal order.

In 2014 wide reform of consumer sales contract was enacted in Poland[64]. Newly created Consumer Law introduced a cohesive and unified system of regulation for sales contract which covers *inter alia* forms of contracts, waiver rights, information obligation[65]. It is of particular importance that reform unified warranty rules for faulty products encapsulated in the Civil Code and rules originally regulated in the Act on Special Conditions of Consumer Sales which was then replaced by the Consumer Law[66]. Amended rules apply to all contracts regardless of whether these were concluded on distance or not[67].

[60] See detailed analysis in question 1.2.1.

[61] "Cascading nature" [pol. *charakter kaskadowy*] means that various claims are not necessarily mutually exclusive and could be used in a successive sequence.

[62] It can be further argued whether full harmonization blurs the distinction between regulation and directive.

[63] B. Lanckoroński, K. Kuszel, *Opinia na temat...*, pp. 141-142.

[64] T. Czech, *Prawa konsumenta. Komentarz*, Wolters Kluwer 2017, pp. 13-15.

[65] W. J. Katner, *Wstępne uwagi na temat nowych przepisów o ochronie praw konsumenta w zakresie rękojmi i gwarancji przy sprzedaży*, in: D. Karczewska, M. Namysłowska, T. Skoczny (eds.), *Ustawa o prawach konsumenta*, C. H. Beck 2015, p. 265.

[66] Consumer Rights Act [pol. *Ustawa z dnia 30 maja 2014 r. o prawach konsumenta*], Dz.U. 2014 poz. 827 ze zm.

[67] Article 1 of Consumer Rights Act. See A. Rogacka-Łukasik, *Zakres zastosowania ustawy z dnia 30 maja 2014 r. o prawach konsumenta*, Przegląd Ustawodawstwa Gospodarczego (8)2015, pp. 17-25; M.

Implementation of Directive on certain aspects concerning contracts for the online and other distance sales of goods will effectively reverse a large part of this reform and fragment previously unified legal regime[68]. Specifically, Articles 9(1) and 9(3) of the proposed directive provides different regulatory approach than currently existing under Polish law[69]. Additionally, Articles 13(1), and 13(3) of mentioned directive have no equivalent in Polish legal order so their implementation will require introducing new legal tools[70].

Taking this into consideration one can venture a conclusion that European Commission approach is not entirely consistent. On the one hand, the proposal pushes for full harmonisation, but on the other act's scope is limited to distance contracts. Of course, only these contracts are relevant for a digital market, and from this perspective such scope is understandable. However, in author's opinion, the real question is should this issue be looked through the lens of the digital market or rather from the general perspective of sales contracts. In essence, discussed proposal creates parallel legal regimes for distance and non-distance contracts. Full harmonisation is not necessarily bad idea in itself (at least not in principle) but not at the expense cohesion of the of contracts' system[71].

Question 1.2.4.

In author's opinion, this issue consists of three closely interrelated sub-questions. First pertaining to the ability of EU regulation to be smoothly incorporated into national legal order without disrupting legal system's cohesion. The second issue, stemming from the former, focusing over a question whether full harmonisation is optimal in a given circumstances. Finally, third of mentioned issues relates to possibility of cooperation in enforcement between the various Member States[72].

Implementation of Directive 2005/29 concerning unfair business-to-consumer commercial practices in the internal market into Polish legal order provides an instructive case study on the above issues. Office of Competition and Consumer Protection had been tasked to prepare transposition, and decision has been made to implement the directive through a new legislative act [pol. *ustawa*], rather than by amendments to existing regulations[73]. The Office claimed

Maciejewska-Szałas, *Zawarcie umowy poza lokalem przedsiębiorstwa w świetle ustawy o prawach konsumenta*, Gdańskie Studia Prawnicze (2)2016, pp. 251-270.

[68] B. Lanckoroński, K. Kuszel, *Opinia na temat...*, pp. 141-142.

[69] See commentary to analogous provisions in Polish law – Article 560 and Article 561 of the Civil Code: A. Kidyba (ed.), *Kodeks Cywilny...*, pp. 130-144; See also M. Manowska, *Rękojmia i gwarancja...*, pp. 34 et seq.

[70] B. Lanckoroński, K. Kuszel, *Opinia na temat...*, pp. 141-142.

[71] See further analysis in question 1.2.4.

[72] Possibility is used in a broad sense encompassing both political will and legal mechnisms.

[73] J. Szwaja, A. Tischner, *Implementacja dyrektywy 2005/29/WE o zwalczaniu nieuczciwych praktyk handlowych do prawa polskiego*, Monitor Prawniczy (20)2007, p. 1119 et seq.

that regulating unfair market practices in one act is consistent with the principles of transparency and clarity, especially given that directive required full harmonisation[74].

This approach had been criticised by the Legislation Council – Government's advisory body[75]. The Council argued that introducing a new legislative act would disrupt the cohesion of pre-existing regulation[76]. There is salient point in this line of reasoning because European lawmakers were influenced by domestic legal systems that have a clear division of B2B and B2C rules[77]. So the introduction of this model into national legal system of States with unified rules for B2B and B2C will inevitably encroach on well-entrenched domestic legal traditions[78]. As a result national legislators, and courts in the Member States could encounter practical interpretative problems[79]. Especially given that serious doubts prevail on the status of general clause [pol. *klauzula generalna*] encapsulated in Article 3(1), which in the original wording of the Directive 2005/29 establish B2C scope[80]. It can be argued (and the case law of national courts seems to confirm it) that mentioned provision *de facto* falls outside full harmonisation requirement as it applies to all "unfair market practices" [pol. *nieuczciwe praktyki rynkowe*], not necessarily those explicitly listed in the directive, and additionally could cover the situation when an unlawful activity is simultaneously directed at customers and competitors[81].

[74] Impact assessment *Uzasadnienie rządowego projektu ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym* [*Substantiation of Government's draft project of Act on combatting unfair market practices*], druk sejmowy 1682 is available at: ww2.senat.pl/k6/dok/sejm/036/1682.pdf (27.04.2017).

[75] A. Kunkiel-Kryńska, *Metody harmonizacji prawa konsumenckiego w Unii Europejskiej i ich wpływ na procesy implementacyjne w państwach członkowskich*, LEX Wolters Kluwer business 2013, p. 359.

[76] Legislation Council's impact assessment *Opinia o projekcie ustawy o zwalczaniu nieuczciwych praktyk handlowych z dnia 22 stycznia 2007 r.* [*Opinion of the draft of January 22nd 2007 on the act on combatting unfair market practices*], RL-0303-138/06 available at: http://radalegislacyjna.gov.pl/dokumenty/opinia-z-22-stycznia-2007-r-o-projekcie-ustawy-o-zwalczaniu-nieuczciwych-praktyk (27.04.2017).

[77] R. Skubisz, *Cele i zakres zastosowania ustawy o zwalczaniu nieuczciwej konkurencji. Dylematy trudnego sąsiedztwa z ustawą o przeciwdziałaniu nieuczciwym praktykom rynkowym*, in: T. Skoczny (ed.), *Prawo konkurencji, 25 lat*, Wolters Kluwer 2016, pp. 576-579.

[78] See also analysis in question 1.2.7. The European legislators seems to be oblivious to the fact that some domestic legal systems have an unified notion of unlawful business practices which covers both acts of unfair competition (B2B), and unfair market practices (B2C). See further M. Pajor, *Harmonizacja prawa prywatnego z prawem Unii Europejskiej*, in: M. Safjan (ed.), *System prawa prywatnego. Tom I*, C.H. Beck 2012, pp. 234 et seq.

[79] E. Łętowska, *Prawo umów konsumenckich*, C.H. Beck 2002, s. 219; R. Stefanicki, *Ustawa o przeciwdziałaniu nieuczciwym praktykom rynkowym. Komentarz*, LexisNexis 2009, pp. 15 et seq.

[80] The wording of this provision was transposed directly into Article 4(1) of the Act on Counteracting Unfair Market Practices.

[81] See *inter alia* Judgments of the Court of Appeal in Katowice, 24.06.2016, V ACa 562/15; 22.01.2016, I ACa 648/15; of the Supreme Court, 16.04.2015, III SK 24/14; of the Court of Appeal in Warsaw, 20.01.2015, VI ACa 457/14; of the District Court in Koszalin [pol. *Sąd Okręgowy*], 27.06.2012, VII Ca 364/12; of the

There are practical merits of this approach, but at the same, it runs contrary to the nature of full harmonisation[82].

Furthermore, to avoid the allegation of incorrect implementation, national lawmakers are essentially limited to the literal transposition of Directive's wording[83]. The judgment of the Court of Appeal in Katowice is especially instructive here[84]. The court held that full harmonisation does not leave any "room for manoeuvre" for national lawmakers when it comes to material law provision, and only procedural matters are left for domestic authorities[85]. According to court, this stems directly from the full harmonisation requirement. At first glance, it looks like the Court of Appeal confused harmonisation with unification, but in this case distinction between these two concepts is *de facto* largely semantic[86].

The problem of cohesive implementation throughout the EU immediately become apparent since mentioned directive extensively uses superfluous and imprecise terminology[87]. Numerous referrals to blurred notions such as "appropriate" [pol. *właściwe*], "professional diligence" [pol. *staranność zawodowa*], or "reasonable" [pol. *racjonalny*] necessitates extensive interpretative guidance through case-law[88]. It then goes without saying that approaches towards interpretation will vary among the Member States with obvious detriment to harmonisation.

Competition Court [pol. *Sąd Ochrony Konkurencji i Konsumentów*], 10.06.2010, XVII AmA 124/09. See also A. Kunkiel-Kryńska, *Metody harmonizacji prawa...*, pp. 369-379.

[82] R. Skubisz, *Klauzule generalne w prawie o zwalczaniu nieuczciwej konkurencji*, Annales Universitatis Mariae Curie-Skłodowska. Sectio G – Ius 63(2)2016, pp. 71-92.

[83] A. Kunkiel-Kryńska, *Metody harmonizacji prawa...*, pp. 371. See on comparable transposition mechanism in J. Szwaja (ed.), *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*, C.H. Beck 2016, p. 728.

[84] Judgment of Court of Appeal in Katowice, 02.12.2010, V ACa 410/10

[85] Analogous interpretation *inter alia* in judgments of Voivodship Administrative Court in Białystok [pol. *Wojewódzki Sąd Administracyjny*], 17.03.2009, I SA/Bk 41/09; of the Supreme Administrative Court in Warsaw [pol. *Naczelny Sąd Administracyjny*], 17.09.2008, II GSK 331/08; 25.11.2009, II GSK 203/09; 08.07.2009, II GSK 1111/08; 31.05.2011, II GSK 522/10; 31.05.2011, II GSK 523/10; 04.11.2011, VI SA/Wa 1786/11; 04.11.2011, VI SA/Wa 1527/11; 31.05.2011, II GSK 611/10; of the Voivodship Administrative Court in Olsztyn, 01.12.2010, I SA/Ol 683/10.

[86] The court is by no means isolated in this opinion. There is considerable body of doctrine's acquis on private law's harmonisation and on drawbacks of full harmonisation model. See *inter alia* Z. Radwański, *Kodyfikacja polskiego prawa cywilnego na tle harmonizacji prawa prywatnego w Unii Europejskiej*, in: W. Czapliński (ed.), *Prawo XXI wieku. Księga Pamiątkowa 50-lecia INP PAN,* INP PAN 2006; E. Łętowska, *Prawo europejskie inspiracją dla dogmatyki prawa cywilnego* , Studia Prawnicze (3-4)2001; E. Łętowska, *Europejskie prawo umów konsumenckich*, C.H. Beck 2004; M. Jagielska, K. Lis, E. Łętowska, P. Mikłaszewicz, A. Wiewiórowska-Domagalska, *Implementacja prawa konsumenckiego w Polsce*, Europejski Przegląd Sądowy (12)2006; F. Grzegorczyk, *Niedoskonałość dyrektyw jako aktów wspólnotowego prawa pochodnego*, Przegląd Ustawodawstwa Gospodarczego (11)2008.

[87] See especially Articles 1(e); 1(h); 2(e); 5(2)b; 5(3); 9(c); 9(d) of the Directive 2005/29.

[88] E. Łętowska, *Dialog i metody. Interpretacja w multicentrycznym systemie prawa*, Europejski Przegląd Sądowy (11)2008; P. Mikłaszewicz, *Antynomie paradygmatu ochrony konsumenta przez informacje – Prawo Unii Europejskiej a prace nad nowym polskim Kodeksem Cywilnym*, in: M. Jagielska, E. Rott-Pietrzyk, A.

Such inconsistency cannot be fully alleviated through pro-EU interpretation without sufficient clarity on the EU level which is not the case here since the wording of directive is vague[89]. CJEU's jurisprudence could offer such needed guidance but first, it must be sufficiently consistent and extensive, and second it puts a strain on national courts operating under continental law models whose are less used to draw from existing case-law[90]. It does not necessarily mean that national court's interpretation done through the lens of preconceived domestic notion will run contrary to Directive's *ratio legis*[91]. Indeed, the problem will be non-existent if these domestic concepts are consistent with these of the EU law, but this cannot be guaranteed[92]. Additionally, the necessity of referral to CJEU case-law could potentially lead to the devolution of national court's competences[93].

It can be claimed that from legislative technique's standpoint vague formulation of mentioned directive is inconsistent with the very nature of full harmonisation[94]. It is, therefore, reasonable to postulate that European lawmakers avoid as much as possible ambiguous terminology whenever they are opting for full harmonisation[95]. However, it is arguable whether attaining this postulate is possible at all. It can be reasonably contended that competition law (both public and private) require a high degree of flexibility, so general clauses are generally needed, but these not sit well with full harmonisation[96].

As of third of the mentioned issues, the European Commission in its 2008 report emphasised the importance of cease-and-desist mechanisms introduced into every domestic legal order as a result of full harmonisation[97]. This Europe-

Wiewiórka-Domagalska (eds.), *Kierunki rozwoju europejskiego prawa prywatnego: wpływ europejskiego prawa konsumenckiego na prawo*, C.H. Beck 2012.

[89] Pro-EU interpretation of national law have its limitations. See *inter alia* A. Sołtys, *Obowiązek wykładni prawa krajowego zgodnie z prawem unijnym jako instrument zapewniania efektywności prawa Unii Europejskiej*, LEX Wolters Kluwer business 2015; K. Kowalik-Bańczyk, *Prowspólnotowa wykładnia prawa polskiego*, Europejski Przegląd Sądowy (3)2005, pp. 16-18.

[90] It by no means implies the lack of sufficient expertise of the national courts, but refers to the lack of well-established tradition, and thus indicates a need for a time consuming adjustment. E. Łętowska, *Dialog i metody. Interpretacja...*, p. 8.

[91] P. Mikłaszewicz, *Antynomie paradygmatu ochrony...*, p. 218; R. Stefanicki, *Klauzula dobrych obyczajów jako kluczowa konstrukcja w ustawie o zwalczaniu nieuczciwej*, Prawo Spółek (7-8)2000, pp. 56 et seq.

[92] A. Kunkiel-Kryńska, *Metody harmonizacji prawa...*, pp. 372-373.

[93] E. Łętowska, *Interpretacja a subsumpcja zwrotów niedookreślonych i nieostrych* Państwo i Prawo 7-8(2011), pp. 17-29.

[94] J. Szwaja (ed.), *Ustawa o zwalczaniu...*, p. 728.

[95] A. Kunkiel-Kryńska, *Metody harmonizacji prawa...*, p. 370.

[96] E. Łętowska, *Dialog i metody. Interpretacja...*, p. 8; E. Łętowska, *Interpretacja a subsumpcja...*, pp. 17 et seq.; P. Mikłaszewicz, *Antynomie paradygmatu ochrony...*, p. 218; R. Stefanicki, *Klauzula dobrych obyczajów...*, p. 56.

[97] Report from the Commission concerning the application of Directive 98/27/EC of the European Parliament and of the Council on injunctions for the protection of consumers' interest, COM(2008)756 final.

wide mechanism of preventive control, according to the Commission, could help combatting cross-border unfair market practices. Presented official optimism seems to be unfounded as procedural rules remain within the domain of national law, so enforceability remains problematic. It is further exacerbated by the mentioned lack of harmony in interpretations of general notions among the Member States. So apart from procedural issues, cooperation suffers from a lack of legal certainty[98]. As a result number of cases on cross-border infringements in negligible[99].

To sum up, full harmonisation in the discussed sphere did not quite build to a satisfying conclusion. The core problem lies with the incompatibility between this model of harmonisation and inevitably vague and open-ended notions required in competition rules. The general direction of European legislative measures is laudable, but minimum harmonisation seems to be less problematic in practice. Alternatively (and purely theoretically) a full-fledged unification can be considered, but this is doubtful from the division of competences' perspective[100].

Question 1.2.5.

At the beginning, it has to be noted that the actual appropriateness of existing regulation and people's confidence in these rules are of course interlinked but nevertheless separate issues[101]. Additionally, it has to be mentioned that rules in themselves cannot be assessed in any meaningful way without analysis of both legal and practical dimension of enforcement. However, it must be clearly emphasised that all jurisdictions of consumer protection have inherent limitations. These must be acknowledged. Apart from purely law-related, these seeming constraints stem from a lack of customers' awareness and inadequacies of enforcement. In author's opinion assessing overall efficiency of consumer protection (in various aspects) and proposing legal solutions lawmakers on both national and European level must be careful not to go beyond of what is not only feasible but practically possible. Creating dead-letter regulations inevitably led to the erosion of confidence in the legal system thus, in the long run, decreasing hte overall level of customer protection.

In author's opinion existing regulations do not display any glaring systemic flaw. Of course, this cannot be understood as a statement that there is no room

[98] R. Stefanicki, *Prawo uczciwej konkurencji a ochrona konsumentów w świetle ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym*, Monitor Prawniczy (2)2011, pp. 63 et seq.

[99] Ibidem.

[100] Opinion on unification's advantage over harmonisation in the sphere of consumer law expressed in J. Maliszewska-Nienartowicz, *Ewolucja ochrony konsumenta w europejskim prawie wspólnotowym*, TNOiK 2004, pp. 27-28. See also R. Stefanicki, *Prawo uczciwej konkurencji a ochrona konsumentów w świetle ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym*, Monitor Prawniczy 1(94)2008, pp. 36-69.

[101] See analysis in question 1.4.6.

for further improvement. However, the controversial issues presented above demonstrates that problems lie with enforcement. In the age of world wide web territorial scope of various legal regulations presents a real obstacle. However, these cannot be overcome trough EU's unilateral measures but rather through international cooperation which is difficult in itself due to various chiefly political factors.

Question 1.2.6.

Under Polish law internet providers' terms and conditions constitute so-called "Contract template" or "contract model" [pol. *wzorzec umowny*][102]. In practice, a person willing to buy some goods online have no impact on the terms of sale and have to accept sellers' rules. Therefore legislator introduced guarantee mechanism encapsulated in Article 385^1(1) of the Civil Code which states: "Provisions of the contract concluded with the consumer are not binding if not individually agreed upon, when creates rights and obligation in a manner contrary to good practices, manifestly infringing consumer's interests (unlawful contract template)"[103].

Since 2016 streamlining of enforcement procedure Office of Competition and Consumer can decide whether a given provision in a consumer contract is abusive [pol. *klauzule abuzywne*, *niedozwolone wzore umowne*] (before it could've been done only through court's procedure) – See detailed analysis in Question 1.4.4[104].

In recent years, there have been numerous cases in Polish courts against electronic service providers where their terms and conditions had been scrutinised[105]. On the basis of Polish competition courts' case-law it is possible to compile a (non-exhaustive) list of most common illegal clauses in online providers' terms and conditions:

[102] The term „Customer Contract Template" [pol. *wzorzec umowy konsumenckiej*] do not have legal definition. The Civil Code in Article 384(1) outlines basic building blocks of these templates: it is set by one of parties, and it could have form of contract pattern or terms and conditions. Therefore, term in question will denote statement of intend on sales of goods/services which is not individualized, but stipulates that potentially unlimited number of contracts could be concluded on the basis of this template. See *inter alia* M. Bednarek, *Wzorce umów w prawie polskim*, C.H. Beck 2005, p. 3; Z. Radwański, *Zobowiązania – część ogólna*, C.H. Beck 2004, p. 142; M. Safjan, *System Prawa Prywatnego. Drugie Wydanie*, C.H. Beck 2012, p. 220; A.M. Zachariasiewicz, *Niektóre problem prawne związane z korzystaniem z nienormatywnych wzorców umownych*, Rejent (9)1995, p. 122.

[103] G. Bieniek (ed.), *Komentarz do Kodeksu Cywilnego*, C.H. Beck 2002, p. 128, 485; B. Gnela, *Umowa konsumencka w polskim prawie cywilnym i prywatnym międzynarodowym*, LEX Wolters Kluwer business 2012, p. 132.

[104] Reform was introduced through The Act of August the 5th 2015 on Amendment of Act on Competition and Consumers Protection and Other Acts [*Ustawa z dnia 5 sierpnia 2015 r. o zmianie ustawy o ochronie konkurencji i konsumentów oraz niektórych innych ustaw*], Dz.U. 2015 poz. 1634.

[105] There is no official statistics compiled with "online providers' terms and conditions" keywords.

- In the absence of payment of the subscription fee the operator reserves the right to disconnect the DDI service until overdue fees are paid during this time current fees are continuously billed[106];
- Subscription fee is non-refundable[107];
- Service provider is not liable for network speed[108];
- In case of service suspension, and service interruption subscription fee is due[109];
- Service provider is not liable for customer data loss and its potential consequences[110];
- Service provider is not liable for subcontractor's network failures[111];
- Seller reserves right to change terms and condition without giving reasons and without prior notice[112];
- All disputes resulting from the sale contract in online store will be settled in the court competent according to the seller's domicile[113];
- In case of contract cancellation paid subscription fee will not be refunded[114];
- Registering an account in the online store amounts to acceptance of processing of personal data for marketing purposes, including sending marketing information to the site's administrator[115].

Additionally, in case-law of Polish courts, there had been some cases when terms and conditions of online service providers did not contain any outright abusive clauses but were vague and thus allowed for an arbitrary interpretation[116].

[106] No. 422, registration date 05.05.2005, case XVII Amc 40/04.
[107] No. 589, registration date 10.03.2005, case XVII Amc 81/04.
[108] No. 638, registration date 19.04.2005, case XVII Amc 23/05.
[109] No. 600, registration date 17.10.2005, case XVII Amc 75/04.
[110] No. 3651, registration date 21.08.2012, case XVII AmC 5354/11.
[111] No. 636, registration date 19.04.2005, case XVII Amc 23/05.
[112] No. 4402, registration date 03.04.2013, case XVII AmC 3325/12.
[113] No. 409, registration date 05.05.2005, case XVII AmC 59/04, and similarly No. 5225, registration date 28.08.2013, case XVII AmC 2186/10.
[114] No. 626, registration date 30.08.2005, case XVII Amc 109/05, similarly no. 486, registration date 25.05.2005, XVII Amc 81/05. See K. Szczygielska, *Odstąpienie od umowy zawartej na odległość w prawie niemieckim i polskim*, Kwartalnik Prawa Prywatnego (2)2003, p. 420.
[115] No. 3522, registration date 5.09.2008, case XVII AmC 341/07. Similarly, in judgment 04.10.2011, XVII AmC 2722/10 confirmed by the Court of Appeal in Warsaw in judgment 14.06.2012, ACa 206/12. The Courts consistently held that agreement regarding sending information for marketing purposed must be expressed separately and must be clearly distinguished from the acceptance of primary contract.
[116] See inter alia Judgment of Regional Court in Warsaw, 30.03.2016, GC 3901/14; of Regional Court in Kalisz 30.03.2016, V GC 833/15.

Question 1.2.7.

In Poland similar mechanism *de facto* already exists. There are two parallel, and complementary mechanisms of combating unfair market practices – public-law-based and private-law-based: Former functions on the basis of Act on Competition and Customer Protection. The material law provisions are closely based on Article 101 and 102 TFEU, and the independent competition authority is responsible for enforcement[117]. Individual undertakings cannot directly go to court against other professional entity on the basis of this act but can request it from the competition authority which is ultimately responsible whether to continue with and start infringement procedure or not[118]. Competition authority can also start proceeding on its own initiative[119].

The latter mechanism is private law-based, and consist of two components. First, The Act on Counteracting Unfair Market Practices provides litigation mechanism available only for consumers (natural persons, non-professional)[120]. There is no exhaustive catalogue of unfair market practices, but the Act provides listed examples of *inter alia* misleading, and aggressive market behaviour[121]. This mechanism does not involve any intermediating organ and the proceeding could be started by an individual, or by consumer protection's organisation as well as by the Consumer Ombudsman or the Ombudsman[122]. The second component of the civil-law-based mechanism consist of the Act of Combating Unfair Competition. Material scope and criteria of prohibited behaviour arevirtually identical in these two private law instruments; the only difference is that the latter is designed for B2B relations[123].

[117] K. Kohutek, M. Sieradzka, *Ustawa o ochronie konkurencji i konsumentów: komentarz*, Wolters Kluwer 2008; T. Skoczny (eds.), *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, C.H. Beck 2014.

[118] K. Róziewicz-Ładoń, *Postępowanie przed prezesem Urzędu Ochrony Konkurencji i Konsumentów w zakresie przeciwdziałania praktykom ograniczającym konkurencję*, LEX Wolters Kluwer business 2011.

[119] Article 10 and 26 of the Act on Competition and Customer Protection.

[120] Article 12(1) The Act on Combating Unfair Market Practices.

[121] M. Sieradzka, *Ustawa o przeciwdziałaniu...*, p. 240. See case-law on interpretation of misleading Competition and Consumer Protection Court cases: 27.02.2012, XVII AmA 192/10; 08.07.2014, XVII AmA 68/12; 11.09.2015, XVII AmA 3/14; 21.07.2016, XVII AmA 10/15; 06.09.2016, XVII AmA 35/16. And on aggressive market practices: Competition and Consumer Protection Court cases 27.03.2015, XVII AmA 142/13; 11.09.2015, XVII AmA 3/14; 11.09.2015, XVII AmA 7/14; 21.04.2016, XVII AmA 25/15; 13.10.2016, XVII AmA 73/14.

[122] The term „interest" [pol. *interes*] in this context is understood as an abstract category – a sum of individual consumers' interest (See Supreme Court Ruling [pol. *uchwała*], 13.07.2006, III SZP 3/06. Similarity with the concept of "collective consumer interest" from the Act on Competition and Customer Protection is apparent.

[123] R. Skubisz, *Cele i zakres zastosowania ustawy o zwalczaniu nieuczciwej konkurencji. Dylematy trudnego sąsiedztwa z ustawą o przeciwdziałaniu nieuczciwym praktykom rynkowym*, in: T. Skoczny (ed.), *Prawo konkurencji, 25 lat*, Wolters Kluwer 2016, pp. 563-579.

To conclude, it is true that small companies dealing with much larger undertakings are often in a disadvantageous position[124]. There are numerous examples of abusive behaviour such as delayed invoice payments, unfavourable contract conditions, and so forth. However, all these activities could be combated under the existing regulation of Act on Combating Unfair Competition and Act on Competition and Customer Protection[125]. It also can be argued that in extreme cases Criminal Law could be used[126]. Thus, expanding the scope of mentioned directive is not necessary.

1.3. Geo-blocking

Question 1.3.1.

Article 1(5) of the draft regulation on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC stated that "This Regulation shall not affect acts of Union law concerning judicial cooperation in civil matters. Compliance with this Regulation shall not be construed as implying that a trader directs his or her activities to the Member State where the consumer has the habitual residence or domicile within the meaning of point (b) of Article 6(1) of Regulation (EC) No 593/2008 and point (c) of Article 17(1) of Regulation (EU) 1215/2012"[127].

It seems that the closest, analytically useful, parallel exist within experiences with E-commerce Directive (2000/31/EC). Further interpretative guidance can also be sought for in CJEU's ruling in *Alpenhof* case and ensuing case law[128]. Indeed, being aware of all *differentia specifica* nevertheless the approach to interpretation of Rome I Regulation and the Brussels I (recast) Regulation invoked by the Court in *Alpenhof* remains relevant for the issue at hand[129]. In mentioned

[124] See inter alia J. Woś, *Korzyści z dualizmu gospodarki rynkowej – małe i średnie przedsiębiorstwa a wielkie korporacje*, Zeszyty Naukowe Wyższej Szkoły Bankowej w Poznaniu (12)1999; E. Mroczek, *Konkurencyjność małych i średnich przedsiębiorstw w gospodarce rynkowej*, Przegląd Organizacji 4/1998.

[125] R. Skubisz, *Cele i zakres...*, pp. 563-579.

[126] This should be considered as a last-ditch solution. In theory Article 286 of the Criminal Code [*Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny*], Dz.U. 1997 nr 88 poz. 553 could be used if unfair market practice, especially misleading could be treated as fraud. Additionally it is questionable whether this could be effective as infringement of law must be proven beyond any reasonable doubt by the prosecution.

[127] Analysis is done on the basis of draft version available at https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-289-EN-F1-1.PDF (15.05.2017).

[128] Case C-585/08, *Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG and Hotel Alpenhof GesmbH v Oliver Heller*, ECLI:EU:C:2010:740.

[129] Especially Article 6(1)(b) Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177, 4.7.2008,

case, the Court elaborated a formula of establishing whether an undertaking is directing its activity to another Member State on the basis of subjective intention to deliver certain services. In other words, assessment should be made if a trader in question "mind to conclude a contract" with the customer in the other Member States[130]. In light of this line of reasoning, one can have certain misgivings whether delimitation simply formulated in quoted Article 1(5) of the draft will function smoothly. A literal understanding of the wording used is contradicting the main interpretative thrust of *Alpenhof* case. If assuming anti-geoblocking rule will come into force, undertakings will be in effect compelled to offer cross-border services and it that case their intentions or state of mind became irrelevant. It is by no means a bad thing in itself, the merely illustrating practical problem with the interpretation of the concept of "directing activities to another Member State". Such interpretative "blurriness" will persist regardless of delimitation clause between the scope of draft regulation and Regulation 1215/2015, and therefore it is likely that new rules will share experiences of E-commerce Directive.

1.4. Questions related to the collaborative economy

Question 1.4.1.

There are few strictly legal problems with the collaborative economy/sharing economy [pol. *gospodarka dzielenia się*, *gospodarka współdzielenia*, although in Poland English terms are sometimes also used]. There is little (but growing) awareness as to what is the meaning of the concept, and collaborative business model is not yet especially popular in Poland[131]. Looking the at Polish legal order through the lens of the main issues raised by the European Commission in its 2016 communication A European agenda for the collaborative economy following observations can be made:

Market access: The Commission expressed the view that entities engaged in sharing economy should have administrative burden of licensing, obtaining

p. 6–16 and Article 17(1)(c) of the Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 01 , 16.01.2001 p. 1-23.

Latter act was replaced by the Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 351, 20.12.2012, p. 1–32 but previous regulation will apply to proceedings instituted before Regulation 1215/2012 comes into application on January 10th 2015.

[130] Case C-585/08 *Alpenhof*, para 76.

[131] I. Rudawska, *Ekonomia dzielenia się, czyli konsumpcja współdzielona i inne formy alternatywnego dostępu do dóbr*, (254)2016 Studia Ekonomiczne, pp. 181-189. It is likely (although data is not entirely conclusive) that observable growth of sharing economy businesses in Poland its primarily savings-driven rather than caused by a specific lifestyle choice.

permissions to facilitate market access limited[132]. So far there have been no attempts to adapt existing regulations to reflect emerging sharing economy activities. However, it has to be noted that in 2013 so-called Deregulation Act [pol. *ustawa deregulacyjna*] had been passed, and then in 2014 Tier II of the Deregulation Act which provides an update to the former act[133]. These acts seek to reduce entry barriers to certain professions, and in some cases completely remove them[134]. These acts had not been enacted with the sharing economy in mind but could help in facilitating market access[135].

Liability: According Commission proposal intermediaries (so-called marketplaces) should be exempted from liability for any damages caused by third parties using their services[136]. At the moment there are no dedicated rules for liability for shared economy. Entities active in this field falls under generic rules encapsulated in the Civil Code[137].

Consumer protection: In Commission's proposal high level of consumer protection should be maintained without imposing unreasonable burdens on persons

[132] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of Regions. A European agenda for the collaborative economy, Brussels, 2.6.2016, COM(2016) 356 final (hereinafter Collaborative Economy Communication), para. 2.1.

[133] *Ustawa z dnia 13 czerwca 2013 r. o zmianie ustaw regulujących wykonywanie niektórych zawodów*, Dz.U. 2013 poz. 829 (Tier I Deregulation Act); *Ustawa z dnia 9 maja 2014 r. o ułatwieniu dostępu do wykonywania niektórych zawodów regulowanych*, Dz.U. 2014 poz. 768 (Tier II Deregulation Act). Currently (06.04.2017) Tier III Deregulation is being prepared. Draft is available at the Government's Legislation Centre [pol. *Rządowe Centrum Legislacji* – RCL] website at: https://legislacja.rcl.gov.pl/docs//2/12283753/12344502/dokument222804.pdf (06.04.2017).

[134] See *Government's Draft of Act on Amendment of Laws Governing Certain Professions* [*Rządowy projekt ustawy o zmianie ustaw regulujących wykonywanie niektórych zawodów*], Druk 806, RM 10-94-12; *Government's Draft of Act on Facilitating Access to Certain Regulated Professions* [*Rządowy projekt ustawy o ułatwieniu dostępu do wykonywania niektórych zawodów regulowanych*], Druk 1576, RM 10-53-13.

[135] See also I. Kawka, *Gospodarcza działalność usługowa w prawie polskim w świetle unijnych swobód przedsiębiorczości i świadczenia usług*, LEX Wolters Kluwer business 2015.

[136] Although liability issues are largely harmonized as online platform's activities falls under regime laid down in E-Commerce Directive (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, p. 1–16) see further analyses in Section 1.1.

[137] See Commentary to Article 353(1) of the Civil Code. Generic definition of obligation encapsulated in this provision is fully applicable to any possible activity in the sphere of sharing economy A. Kidyba (ed.), *Kodeks Cywilny. Tom II, Zobowiązania*, LEX, Wolters Kluwer business 2014, p. 23-28; A. Olejniczak (ed.), *System Prawa Prywatnego. Tom 6, Prawo zobowiązań – część ogólna*, C.H. Beck 2014, p. 120; Parties are free to create the nature of their contractual relationship (Article 353^1 of the Civil Code). See Z. Radwański (ed.), *System Prawa Prywatnego. Tom 2, Część Ogólna*, C.H. Beck 2008, p. 177; K. Pietrzykowski (ed.), *Kodeks cywilny. Komentarz, tom 1*, C.H. Beck 2011, p 1261. The provision must be defined otherwise the obligation is void (See Supreme Court's ruling, 01.04.2011, III CSK 206/10) which is not the case in sharing economy even if a given service is non-professional, sporadic and possibly *ad hoc*.

only occasionally acting as service providers. Currently in Polish law "consumer" [pol. *konsument*] is defined as an individual (only natural person) entering into a contract [pol. *czynność prawna*] with an entity professionally engaged in economic activity[138]. The situation with sharing economy is problematic in this respect as an individual is directly engaged with another person who is only occasionally providing certain service, and not always for-profit. It is a common practice for subcontractors to register their economic activity under self-employment rules [pol. *jednoosobowa działalność gospodarcza*][139]. Such maneuver solves both liability and customer protection issues in a manner where an actual supplier could be held liable, but it imposes a severe administrative burden on an individual so it is ill-suited for incidental activity[140]. Another legal relationship exists between the recipient of service and go-between, because where are no doubts the latter is a professional entity, but the subject of this obligation is limited to intermediary services. As a result, there are two separate legal obligations regarding liability – for intermediary services, and for the supply of the actual service. Regardless, despite these doubts, there are hardly any complaints about the insufficient level of customer protection as a result of undertakings operating according to sharing economy model[141].

Employment: The Commission's proposal emphasises the need to provide the rules for establishing the legal status of persons working in and for online intermediary platforms[142]. In principle, the rules governing employment law are within the sphere of State's competences therefore little what can be done on the EU level apart from some general guidelines. Currently, in Poland, there are two main methods of regulating legal status of mentioned individuals. Former is self-employment. It has already been said that this is primarily suited for persons engaged in a full-time activity (see paragraph above). Latter is civil contract [pol.

[138] Article 221 of the Civil Code. This contract cannot be related to individual's economic or professional activity nor it can be profit driven. See J. Haberko, *Umowa sprzedaży konsumenckiej zawarta poza lokalem przedsiębiorstwa*, Przegląd Sądowy (3)2007, p. 98; S. Koroluk, *Nowa definicja konsumenta w Kodeksie Cywilnym*, Radca Prawny, (6)2003, p. 26.

[139] In Poland this form of economic activity is functioning on the basis of Article 43^1 and Article 43^4 of the Civil Code and Act on the Freedom of Economic Activity [*Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej*], Dz.U. 2004 nr 173 poz. 1807. See further A. Powałowski, *Firma osoby fizycznej*, Gdańskie Studia Prawnicze, (XXIX)2013, pp. 171-180.

[140] Individuals wishing to register an economic activity are required to submit CEIDG-1 form (application for entry into the Central Registration and Information on Economic Activity), and obtain tax identification number REGON and NIP. Procedure is relatively straightforward but it hard to imagine anyone planning to provide given service only few times during large timespan would be willing to go through these steps.

[141] See analysis of Uber case in question 1.4.2.

[142] Collaborative Economy Communication, para 2.4.

umowa zlecenie][143]. It has been primarily designed to regulate freelancing and thus is appropriate for sharing economy[144]. The legal construction of it looks as follows: intermediary (online platform) concludes a civil contract with a person who in turn is offering service to end-users on behalf of this online platform uder separate contract[145]. In all cases, pre-existing legal tools are utilised, and there are no legislative initiatives to enact dedicated solutions for the collaborative economy.

Taxation: The Commission's Communication does not provide any guidance on this issue (in any case direct taxation is the sphere of State's exclusive competence) and limits itself to very vague statement that this matter should be regulated to prevent tax avoidance[146]. Polish Ministry of Finance expressed view that there is no need to create dedicated rules on taxation for collaborative economy[147]. According to Ministry activity in question is nothing else than a contract between service provider and recipient of service concluded through an online platform. Under Polish law, every natural person is individually responsible for paying all taxes for relevant taxable income[148]. However, the situation is far from clear as under existing regulations individual's income could fall under various tax rates depending on its categorization[149]. Additionally, if an individual's activity could

[143] Articles 734-751 of the Civil Code are applicable. In principle. Individuals bound by the contract in question are not employees and thus are outside the scope of the Labour Code [*Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy*], Dz.U. 1974 nr 24 poz. 141 ze zm. Most rules governing these contracts are *ius dispositivum* (see Supreme Court's judgment [pol. *Sąd Najwyższy*], 23.11.2011, IV CNP 14/11) therefore the legal instrument in question offers significant flexibility.

[144] J. Rajski (red.), *System prawa prywatnego. Tom 7, Zobowiązania – część szczegółowa*, C.H. Beck 2011, s. 561; E. Gniewek, P. Machnikowski, *Kodeks Cywilny Komentarz*, C.H. Beck 2013, pp. 1263–1264.

[145] In principle individual being a party to a contract in question is liable for its fulfilment (K. Osajda (ed.), *Tom III B. Kodeks cywilny. Komentarz. Zobowiązania. Część szczegółowa. Ustawa o terminach zapłaty*, C.H. Beck 2016, p. 1494). In certain situation a substitute could be appointed, and then both substitute and the party could be jointly held liable [pol. *odpowiedzialność solidarna*] (Supreme Court's judgment 19.08.1971, I CR 300/71, OSN 1972, nr 4, poz. 70). Substitution will never be possible in employment relationship. (Supreme Court's judgment 02.12.1998, I PKN 458/98). It is possible for a mentioned contract to be reciprocal. In this case one side would provide intermediary services while other the actual service that is being advertised. In case-law in such situations provisions of Civil Code dedicated for reciprocal obligations are applicable – Article 491(1) of the Civil Code (See Supreme Court's judgment, 24.10.2000, V CKN 135/00) and Article 494 of the Civil Code (See Supreme Court's judgments, 28.11.2008, V CSK 215/08; 29.02.2008, II CSK 463/07). It stands to reason that a separate legal relationship exist between latter party and the end-users.

[146] Collaborative Economy Communication, para 2.5.

[147] This policy statement has been expressed twice 26.02.2015 and 01.06.2015 in replies to interpellation of MP Zbigniew Chmielowiec (nos. 30845 and 32705).

[148] Article 9(1) of the Personal Income Tax Act [*Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych*], Dz.U. 1991 nr 80 poz. 350 ze zm. with the exemptions provided in Articles 21, 52, 52a and 52c of mentioned act.

[149] These can be: Individual activity – civil contract; contract of commission concluded with a person carrying out an economic activity (Article 13 of the Personal Income Tax Act); non-agricultural economic

be considered as being economic, only income above tax deductible expenses is taxable[150]. If a person who is sharing certain item is receiving income that is not higher than costs typically incurred by the maintenance of this item, there are no grounds for taxation[151]. Furthermore, certain sharing services could be classified as "Lending Agreement" [pol. *umowa użyczenia*] which stipulates that user of a given item be required to bear its operating costs[152]. It goes without saying that these agreements are non-taxable[153]. As of indirect taxation, 2015 proposition of changes to VAT Directive are to be commended for creating fairer rules for online marketplaces (taxation on the basis of income's place)[154]. There is persisting issue of taxation of individuals' sharing certain goods. Even if a person is providing a service in a continuous manner and for profit, it can still benefit from individual tax exemption [pol. *zwolnienie podmiotowe*][155]. It can be problematic from a competition standpoint as exempted individual will have much lower operating costs[156]. It is because a professional entity employing a number of individuals actually providing given service (although from a legal standpoint the undertaking is providing service and those individuals are just employed) is being taxed on the basis of the total, aggregated income[157]. If on the other hand, these individuals are working on their behalf, their income is naturally lower,

activity (Article 14 of the Personal Income Tax Act); Rent, lease, and other agreements of similar (Article 16b of the Personal Income Tax Act); other sources of income (regulated by title XXI of the Civil Code).

150 Article 9(2) in relations to Article 11(1), Article 23 and Article 22(1) of the Personal Income Tax Act.

151 Interpretation firmly established in case law. See judgment of Supreme Administrative Court 09.10.2002, I SA/Wr 1118/00, POP 2003, z. 2, s. 33; 2.02.2002, SA/Sz 43/00; and of Voivodship Administrative Court in Gliwice, 25.06.2008, I SA/Gl 79/08. See also A. Bartosiewicz, R. Kubacki, *PIT. Komentarz, Wydanie V*, LEX Wolters Kluwer business 2015, pp. 565-635.

152 Article 713 of the Civil Code. See further J. Panowicz-Lipska (red.), *System prawa prywatnego. Tom 8, Zobowiązania – część szczegółowa*, C.H. Beck 2011, s.; E. Gniewek, P. Machnikowski, *Kodeks Cywilny...*, pp. 1246.

153 Although fact that lender is not required to bear usual operating cost of an item is considered to be an "advantage" [pol. *korzyść*] for tax and insurance purposes. See judgment of the Court of Appeal in Warsaw, 27.03.2013, I ACa 1166/12.

154 Proposal for a Council Directive amending Directive 2006/112/EC on the common system of value added tax as regards the temporary application of a generalised reverse charge mechanism in relation to supplies of goods and services above a certain threshold, COM/2010/0331 final – CNS 2010/0179.

155 Allowed under Article 113 of the Law on VAT [*Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług*], Dz.U. 2004 nr 54 poz. 535 ze zm. See D. Dominik-Ogińska (ed.), *Zwolnienia w zakresie podatku od towarów i usług. Komentarz*, Wolters Kluwer 2016.

156 Downward pressure on costs is generally positive, here the concern is that competitive edge is not achieved on a level playing field.

157 Depending on the legal status of an economic activity it could be taxable under Personal Income Tax Act or Corporate Income Tax Act [*Ustawa z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych*], Dz.U. 1992 nr 21 poz. 86 ze zm.

and thus tax basis goes down[158]. To sum up, in Poland, there are neither dedicated tax rules for collaborative economy nor any plans to create such regulations. The official line of the Finance Ministry is that no legislative action is required.

Question 1.4.2.

The most glaring example of competition issue relates to the activity of Uber *versus* registered taxi companies. Uber is operating an online app which allows consumers with smartphones to submit a trip request, which the software program then automatically sends to the Uber driver nearest to the consumer, alerting the driver to the location of the customer. Uber drivers use their own cars. In Poland company's activity is registered as "providing and administering an online platform which allows contact between drivers and customers and process payments"[159]. To provide taxi transport services, a valid license is required. Act on Road Transportation provides a checklist of criteria for obtaining this license[160]. These apply both to owner/operator as well as to employed drivers, and include *inter alia* requirements for specific training[161]. Since 2013 local governments [pol. *samorządy*] are free to decide requirements for obtaining a license[162].

Following complaints raised by numerous taxi companies Office of Competition and Consumer published an official statement explaining its position on the issue[163]. The Office is well aware of the increasing role of sharing economy and concludes that Uber's competitive edge comes from technological advantage, but its activity is not aimed at eliminating competition. Additionally, the Office expressed the view that Uber services are not well-suited for every customer as

[158] Of course tax rates are proportional so in principle should have equal effect regardless of the total amount due, but exemptions in question are threshold-based, so in practice low turnover entities are not taxed.

[159] Uber is registered in National Registry [pol. *Krajowy Rejster Sądowy*] under no. 0000490069 with listed activities „Preparing and Processing data" [pol. *Przygotowywanie i przetwarzanie danych*] (SIC 73740000), and Other IT and Computer technology Services [pol. *Pozostała działalność usługowa w zakresie technologii informatycznych i komputerowych*] (PKD 62.09.Z).

[160] Article 6 of the Act on Road Transportation [*Ustawa z dnia 6 września 2001 r. o transporcie drogowym*], Dz.U. 2001 nr 125 poz. 1371 ze zm.

[161] R. Strachowska, *Ustawa o transporcie drogowym. Komentarz, wydanie III*, LEX Wolters Kluwer business 2012. Local government [pol. *Rada Gminy*](with population more than 100000) can establish additional criteria for obtaining license which may include *inter alia* exam from street topography (Article 6(3) of the Act on Road Transportation). In the era of GPS navigation in author's opinion these additional requirements are unreasonable and should be treated only as a protectionist barriers to entry.

[162] Act on Road Transportation was amended by Article 16 of the Tier I Deregulation Act. It added Article 3a which provides possibility to impose additional requirements for obtaining taxi license.

[163] *Uber – stanowisko UOKiK* [*Uber – Office of Competition and Consumer's position*], Published on 05.05.2016, available on Office of Competition and Consumer website at: https://www.uokik.gov.pl/aktualnosci.php?news_id=12352 (09.04.2017).

they not allow for cash payment and anonymity[164]. In this vein, they are not in the same product market as legacy taxis although an overlap is indisputable.

There is another controversial issue pertaining to the driver's legal status. Under existing regulation, every person providing "carriage by road transport" requires a valid licence regardless whether this activity falls under *lex specialis* of taxi licence or have a different nature (for example coach transport, limo services,)[165]. The ultimate responsibility to obtain such license falls on the person actually providing a service. So since Uber is registered as an online platform administrator from its perspective, it is sufficient to get a declaration that drivers are providing service according to all existing regulations. It goes without saying that hardly any of its drivers had this license but this could only be established during individual control carried out by Road Transport Inspectorate which is problematic in practice since Uber cars are not marked[166]. Since 2016 Uber requires cooperating drivers to register economic activity under self-employment rules[167].

It remains to be established by the road safety authorities whether it is sufficient to maintain an adequate level of safety. From competition from a competition standpoint, Uber is not misleading its customer as to what is the nature of its services and further down the road the actual contract for carriage is concluded between individual drivers and the passenger[168].

The Office concluded that level of customer protection achieved in registered taxis by publishing tariffs and equipping cars with taximeters is no smaller in the case of Uber drivers. The application provides a clear pricing structure, and by ordering a driver, fare is known *ex-ante*. The same holds true for customer complaints. The application contains clear policy, and the complaints could be lodged either through the app or by the phone. The Office additionally stated that it received no complaints on Uber services although it has to be noted, given the relatively small value of fares, it is unlikely that unsatisfied customers would go ahead with official complaints[169].

[164] There is registration requirement and credit card information have to be provided for payment processing which may not be desirable for more privacy conscious customers.

[165] Article 5b of the Act on Road Transportation. At the same time according to Supreme Administrative Court [pol. *Naczelny Sąd Administracyjny*] providing sporadic transport is a separate service from taxi services (judgment 21.10.2009, II GSK 143/09). It can be argued that this line of interpretation applies to most Uber drivers.

[166] On competences of Road Transport Inspectorate [pol. *Inspekcja Transportu Drogowego*] to carry out inspections see R. Strachowska, *Ustawa o transporcie...*, pp. 294 et seq.

[167] Uber terms and conditions applicable for cooperating drivers are available at https://www.uber.com/legal/terms/pl/ (09.04.2016).

[168] *Uber – stanowisko...*

[169] Ibidem.

Another competition issue raised by Uber relates to taxation[170]. The issue has been analysed in detail in question 1.4.1., but from the competition standpoint, it has to be noted that the most contentious issue relates to a potential cost advantage sharing economy operator could achieve. Competitive pressure in principle is a good thing, but competition should be on the level playing field. In this case, one could argue that individuals performing sporadically similar services as professionals should be equally burdened especially regarding taxation. This brings up the question whether the scale of sharing economy undertaking requires any heavy-handed regulatory action. Especially given level of substitutability between individuals operating under the collaborative economy model and "legacy" professionals is arguable[171].

Question 1.4.3.

It is hard to provide a definitive answer as on the one hand no one is keeping track of entities operating under sharing economy model, and in any case, the categorization may be problematic as the notion remains superfluous. On the other hand, the collaborative economy sector is not well developed in Poland so it could be the case that an activity where operating under sharing economy model is possible but so far there are no undertakings active.

Looking at the spheres where collaborative economy undertakings are active in Poland, licenses are required for road transportation services and operating taxis[172]. Additionally, road transport and tourist services require compulsory liability insurance (OC).

In any case, provided given activity will be carried out professionally and with some regularity, generic rules for registering economic activity applies[173]. According to Doing Business Reports published annually by the World Bank in 2017 starting a business in Poland requires on average completing four administrative procedures which take around 37 days, and costs approximately 12.1%

[170] This holds true for all sharing economy activities.

[171] Airbnb serves as a prime example. Despite some superficial similarities there is little actual competition between its services and traditional HORECA businesses.

[172] Formally speaking Uber is not a taxi company. In Poland company is registered in National Court Register [pol. *Krajowy Rejestr Sądowy*] with its primary activity listed as „Preparing and processing data" [pol. *Przygotowywanie i przetwarzanie danych*] SIC 73740000; and „Other business and management consultancy" [pol. *Pozostałe doradztwo w zakresie prowadzenia działalności gospodarczej i zarządzania*], PKD 70.22.Z.

[173] In principle (although there are some exemptions) every economic activity falls under The Freedom of Economic Activity Act [pol. *Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej*], Dz.U. 2004 nr 173 poz. 1807ze zm. establishing generic rules for conducting a business. See also analysis in question 1.4.5.

of individuals' income per capita[174]. This (as of 2017) places Poland at 107 in the ranking of 190 economies. Although this result is far from satisfactory a significant progress has been made since the systemic transformation[175]. However, in most recent years, there is relatively small, but observable reversal[176].

Question 1.4.4.

The wording of this question indicates that it refers to consumer protection in general, not only in the specific context of the collaborative economy but at the same time it is placed in the section dedicated to sharing economy which suggests specific focus. The author decided to take broad approach suggested by the actual wording of the question above, especially given that it is hard to pick issues relevant exclusively for the collaborative economy while most general contentious issues are at least to some degree applicable for sharing economy[177].

While consumer protection issues may not be the principal sphere of current legal debate in Poland, the issue is always present especially in light of the rapid growth of e-commerce. However while existing level of consumer protection can be to a large extent attributed to the European Union and existing standards are considered satisfactory, from this "European" standpoint, the current trend is to enhance the legal protection of micro- and small undertakings.

It does not mean that there are no issues with customer protection but is hard to pick the most glaring problem, and it goes without saying that there are diverse opinions among doctrine on this subject[178]. So the presented issues reflect only the author's opinion.

Definition of "consumer": As been previously mentioned, in Poland, Consumer [pol. *konsument*] is defined in the Civil Code as is a natural person entering into a legal relationship with an entity professionally engaged in economic activity[179]. It is interpreted as containing prohibition to be directly linked with person's

[174] Doing Business Report is available at: http://www.doingbusiness.org/~/media/WBG/DoingBusiness/Documents/Profiles/Country/POL.pdf (15.05.2017) p. 19.

[175] Of the notable initiatives Poland made star ting a business easier by eliminating the requirement to register the new company at the National Labour Inspectorate [pol. *Państwowa inspekcja pracy*] and the National Sanitary Inspectorate [pol. *Główny inspektorat sanitarny*].

[176] For instance in 2017 in comparison with 2016 in category „Starting a Business" Poland dropped five places; in category „Paying Taxes" drop was three places. The overall position dropped from 102 to 107.

[177] Additionally the issue of legal situation of borrowers of mortgages in CHF is especially controversial in Poland both from political and legal standpoint. Due to lack of relevance with the general topic of this report this problem will not be analysed in this paper.

[178] See *inter alia* M. Ganczar, E. Sługocka-Krupa (eds.), *Ochrona konsumentów i jej współczesne*, KUL 2014; T. Skoczny (ed), *Prawo Konkurencji*....

[179] Definition is formulated in the Article 22^1 of the Civil Code.

economic or professional activity[180]. In the sphere of the collaborative economy, a person concluding a trade deal with non-professional is arguably not regarded as consumer although if the other party is acting for profit, the consumer criteria seem to be satisfied[181].

Changes in combating unfair clauses in consumer contracts: Prior April 2016 assessment, whether given contract's clause is abusive/unfair, had been done by a Competition upon complaint from the President of the Office of Competition and Consumer. Once the particular provision was regarded as abusive (unfair terms) it could not be used in future any contracting parties – decision is binding *erga omnes*[182]. Abusive clauses are blacklisted in a dedicated registry [pol. *rejestr klauzul niedozwolonych*][183]. *In toto,* as of 03.04.2017, there are 6938 registered prohibited clauses[184]. This mechanism was sometimes criticised as insufficiently effective especially when it comes to preventive control[185]. The main argument against it what it is too cumbersome as it requires time-consuming court proceeding, and then it is unrealistic to sift through nearly seven thousand clauses (without a search engine) to check whether given clause is abusive or not. In April 2016 the enforcement mechanism has been streamlined[186]. Clauses in consumer

[180] Z. Radwański, *Podmioty prawa cywilnego w świetle zmian kodeksu cywilnego przeprowadzonych ustawą z dnia 14 lutego 2003 r.*, Przegląd Sądowy (7-8)2003, p. 12. There is prevalent opinion (incorrect in the light of CJEU case-law) that if activity is non-profit it is not economic in nature thus an individual engaged in it falls under definition of consumer. See: S. Koroluk, *Nowa definicja konsumenta w k.c.*, Radca Prawny (3)2003, p. 26.

[181] S. Koroluk, *Nowa definicja...*, p. 26.

[182] See Court of Competition and Consumer Protection [pol. *Sąd ochrony konkurencji i konsumentów*] cases 16.11.2005, VI ACa 473/05 (Dz. Urz. UOKiK 2006, nr 2, poz. 35); 02.12.2005, VI ACa 760/05 (Dz. Urz. UOKiK 2006, nr 1, poz. 19). Blacklisted clauses are published in Monitor Sądowy i Gospodarczy. B. Gawlik, *Skutki wyroku w sprawach o uznanie postanowień wzorca umowy za niedozwolony*, Prace Instytutu Prawa Własności Intelektualnej UJ (96)2006, pp. 190-193; M. Jagielska, *Skutki wpisu postanowienia wzorca umownego do rejestru niedozwolonych postanowień*, Europejski Przegląd Sądowy (5)2007, p. 47; M. Michalska, M. Wojewoda, *Kilka uwag o rozszerzonej mocy wiążącej wyroków uznających postanowienia wzorca umowy za niedozwolone*, Radca Prawny (4/5)2008, pp. 27-28.

[183] It is not necessary for a clause to have exactly the same wording as the one registered as prohibited. It is sufficient to be comparable in terms of results. M. Sieradzka, *Ustawa o przeciwdziałaniu nieuczciwym praktykom rynkowym: Komentarz*, Oficyna Wolters Kluwer business, Warszawa 2008, p. 222. See Court of Competition and Consumer Protection [pol. *Sąd Ochrony Konkurencji i Konsumentów*] judgment 25.03.2004, XVII Ama 51/03.

[184] Full list with customizable search engine is available at the Website of Office of Competition and Consumer at: https://www.uokik.gov.pl/rejestr_klauzul_niedozwolonych2.php (03.04.2017).

[185] K. Gajda-Roszczynialska, *Sprawy o ochronę indywidualnych interesów konsumentów w postępowaniu cywilnym*, LEX Wolters Kluwer business 2011, p. 315; M. Sieradzka, *Ustawa o przeciwdziałaniu...*, p. 222; M. Skory, *Klauzule abuzywne w polskim prawie ochrony konsumentów*, Zakamycze 2005, p. 304–308.

[186] Reform was introduced through the Act of August 5th 2015 on the amendment of the Act on Competition and Consumer Protection and other acts [*Ustawa z dnia 5 sierpnia 2015 r. o zmianie ustawy o ochronie konkurencji i konsumentów oraz niektórych innych ustaw*], Dz.U. 2015 poz. 1634.

contracts can be considered as abusive by the decision of President of the Office of Competition and Consumer. It is done through the straightforward administrative proceeding, and there is no longer need for a judicial means[187]. The registry of abusive clauses was replaced by an online database with an extensive search engine[188]. Abusive clauses are listed primarily for information purposes, aiding legal certainty since the previous list was too unwieldy and now blacklisting is done in very prompt manner[189]. Under previous rules, blacklisted clauses were prohibited in future contracts and automatically void which was problematic given a high number of positions in the registry[190]. Offending undertakings could've been fined for imposing terms and conditions containing blacklisted clauses[191]. Under new regulations undertaking using unfair clauses can be immediately fined, requested to annexe offending contracts, and of course, this clause cannot be used in any future contract (decision binds *erga omnes*)[192].

Issues mentioned above are purely legal relating to imperfect regulations. However, the majority of problems with effective consumer protections are not systemic in nature but stemming from a lack of individuals' awareness. It applies in equal measure to the knowledge of customers' rights vis-à-vis undertaking and to knowledge where to look for assistance in case of problems. According to statistics run by the regional offices of customers' ombudsman [pol. *Rzecznik Praw Konsumenta*] the vast majority of complaints lodged relating to issues with warranty for faulty products and returns policy, so something where legal doctrine is generally in agreement that existing rules are containing sufficient safeguards. Having said that is also have to be noted that awareness of consumer rights is steadily growing, so the problem colloquially referred to as "Consumer lost on the Internet" is declining[193].

[187] M. Namysłowska, A. Piszcz (eds.), *Ustawa o zmianie ustawy o ochronie konkurencji i konsumentów z 5.8.*, C.H. Beck 2016, pp. 21-30.

[188] List with extensive search engine is available at https://www.uokik.gov.pl/rejestr_klauzul_niedozwolonych2.php (15.05.2017). Previously the formal requirements for registry of abusive clauses [officially named *rejestr postanowień wzorców umowy uznanych za niedozwolone*] were set out in a Council of Ministers' Regulation *Rozporządzenie Rady Ministrów z dnia 19 lipca 2000 r. w sprawie wzoru rejestru postanowień wzorców umowy uznanych za niedozwolone*, Dz.U. 2000 nr 62 poz. 723.

[189] M. Namysłowska, A. Piszcz (eds), *Ustawa o zmianie...*, pp. 21 et seq.

[190] See *inter alia* analysis J. Nawracała, *Klauzule abuzywne w ubezpieczeniach – wadliwość obowiązującej regulacji*, Prawo Asekuracyjne (4)2010, p. 52; B Wyżykowski, *Abstrakcyjna kontrola postanowień wzorców umów*, Przegląd Prawa Handlowego (10)2013, pp. 30-40.

[191] M. Skory, *Klauzule abuzywne w polskim prawie ochrony konsumenta*, Zakamycze 2005, pp. 298-315.

[192] The same was true prior to amendment but given high number of clauses and difficulty with searching it was problematic in practice.

[193] M. Królikowka-Olczak, B. Pachuca-Smulska (eds.), *Ochrona prawna konsumenta na rynku mediów elektronicznych*, C.H. Beck 2016, pp. 103-115.

Question 1.4.5.

The notion of „entrepreneur" [pol. *przedsiębiorca*] encapsulated in Article 43[1] of the Civil Code [pol. *Kodeks cywilny*] is applicable in principle[194]. According to this definition, an entrepreneur is "a natural person, a legal person, an organisational unit without legal personality, who's law grants legal capacity, which carries out an economic or professional activity on its behalf" [pol. *osoba fizyczna, osoba prawna i jednostka organizacyjna, która nie jest osobą prawną, a której ustawa przyznaje zdolność prawną, prowadząca we własnym imieniu działalność gospodarczą lub zawodową*][195]. Generally, the notion of "entrepreneur" is defined through three sets of criteria: Subjective, functional, and subjective-functional[196]. Former denotes requirement of legal capacity[197]. Functional criterion encapsulates two sub-criteria[198]. The entity must carry out economic activity and must do it on its behalf[199]. Mentioned activity must be conducted in an "organised and continuous manner", and be profit driven[200]. Last criterion linked activity carried own on its behalf with the economic consequences (business risk) of it[201].

[194] There is no direct equivalent of the term "trader" [pol. *kupiec*] in Polish law. This term was historically used in 1934 Trade Code.

[195] See also M. Szydło, *Pojęcie przedsiębiorcy w prawie polskim*, Przegląd Sądowy (7-8)2002, pp. 95 et seq. See ruling of the Supreme Court, 22.08.2003, I PK 284/02, OSNP 2004, nr 17, poz. 29, where Court held that "entrepreneur" relates to natural person engaged in an economic activity, not to all assets used to carry out this activity.

[196] J. Szwaja, *Pojęcie przedsiębiorcy a instytucja prokury (Przedsiębiorca jako podmiot udzielający prokury*, in: A. Nowicka (ed.) *Prawo prywatne czasu przemian. Księga pamiątkowa dedykowana Profesorowi Stanisławowi Sołtysińskiemu*, UAM, 2005, p. 286.

[197] W.J. Katner, *Podwójna czy potrójna podmiotowość w prawie cywilnym* in: W. Popiołek, L. Ogiegła, M. Szpunar (eds.) *Rozprawy prawnicze. Księga pamiątkowa Profesora Maksymiliana Pazdana*, Zakamycze 2005, p. 1031; K. Pietrzykowski (ed.), *Kodeks cywilny. Tom I. Komentarz do art. 1-449(10)*, C.H. Beck 2005, p. 128; E. Gniewek (ed.) *Kodeks Cywilny. Komentarz*, C.H. Beck 2006, p. 95.

[198] A. Kidyba (ed.), *Kodeks cywilny. Komentarz. Tom I. Część ogólna, wyd. II*, LEX Wolters Kluwer business 2012, pp. 209-211.

[199] T. Szanciło, *Przedsiębiorca w prawie polskim*, Przegląd Prawa Handlowego (3)2005, p. 4 et seq. See also ruling of the Supreme Court, 06.12.1991, III CZP 117/91, OSNC 1992, nr 5, poz. 65.

[200] Ruling of the Supreme Court, 30.11.1992, III CZP 134/92, OSCP 1993, nr 5, poz. 79. On the interpretation of the notion of „organized manner" see Z. Radwański, *Prawo cywilne*, LexisNexis 2007, p. 208; M. Pyziak-Szafnicka (ed.), *Kodeks cywilny. Część ogólna. Komentarz*, LEX Wolters Kluwer business 2009 p. 409; W.J. Katner, *Przedsiębiorca i konsument w projekcie księgi pierwszej nowego kodeksu cywilnego – do czego zmierza Komisja Kodyfikacyjna?* in: M. Modrzejewska (ed.), *Prawo handlowe XXI wieku. Czas stabilizacji, ewolucji, czy rewolucji. Księga jubileuszowa Profesora Józefa Okolskiego*, Wolters Kluwer 2010, pp. 377 et seq. And on the notion of „continuous manner" J. Odachowski, *Ciągłość działalności gospodarczej*, Glosa (10)2003, pp. 30 et seq.; J. Frąckowiak, *Instytucje prawa handlowego w kodeksie cywilnym*, Rejent (6)2003, pp. 31 et seq.; M. Safjan (ed.), *System prawa prywatnego. tom I*, C.H. Beck 2012, pp. 1105 et seq.

[201] M. Szydło, *Pojęcie działalności...*, pp. 25 et seq.; M. Safjan (ed.), *System prawa prywatnego...*, pp. 1103. Differently J. Szwaja, *Pojęcie przedsiębiorcy a...*, p. 286 who claims that acting in its own name is not necessarily the same as acting on its own behalf. .; J. Frąckowiak, *Instytucje prawa handlowego...*, pp 34 et seq.; K. Pietrzykowski (ed.), *Kodeks cywilny...*, p. 157.

It is apparent that many individuals active in the collaborative economy fall outside this definition. If a person's activity is sporadic, incidental, not carried out in an "organised and continuous manner" in the meaning of the abovementioned provision, then generic rules of the Civil Code applies[202]. In a nutshell, there is no lacuna, but there are no dedicated regulations either.

Specific regulation exists for timeshare agreements[203]. The term, used in Polish law in its original English version, is defined as a contract under which consumer acquires the right to use an additional place of accommodation during periods specified in the contract[204]. The contract must be signed for at least a year, so the case of individuals swapping houses once a year during a holiday – a popular collaborative economy activity – are likely outside the scope of this regulation due to smaller timespan[205]. So the timeshare rules were not designed with the specific idea of sharing economy in mind but to some extent could be relevant[206].

Question 1.4.7.

The very concept of trust is superfluous and difficult to define. There is an extensive body of research works from the spheres of *inter alia* psychology, behavioural economics tackling various aspects of this concept that cannot be described by a rigid conceptual framework of single scientific discipline[207]. Trust as a perception is highly individualised and subjective as depends on a multitude of cognitive factors. It is accepted that degree of trust in peer-to-peer (P2P) is lower than in "traditional" businesses, but the specific data is inconclusive. It stands to reason that P2P markets are highly heterogeneous and thus it is problematic to collect

[202] A. Kidyba (ed.), *Kodeks cywilny. Komentarz...*, pp. 206-208; Z. Radwański, *Podmioty prawa cywilnego w świetle zmian kodeksu cywilnego wprowadzonych ustawą z dnia 14 lutego 2003 r.*, Przegląd Sądowy (7-8)2003, pp. 22 i n.; M. Jagodziński, *Pojęcie przedsiębiorcy i przedsiębiorstwa w świetle obowiązujących regulacji prawnych*, Przegląd Prawa Egzekucyjnego (2)2011, p. 30.

[203] Creating Rules dedicated to timesharing was necessary due to implementation requirement of the Directive 2008/122/EC of the European Parliament and of the Council of 14 January 2009 on the protection of consumers in respect of certain aspects of timeshare, long-term holiday product, resale and exchange contracts, OJ L 33, 3.2.2009, p. 10–30. K. Ludwichowska, *Dyrektywa UE o timeshare a konieczność reformy prawa polskiego*, Państwo i Prawo (4)2010, p. 70. The directive was implemented by the Timeshare Act [*Ustawa z dnia 16 września 2011 r. o timeshare*], Dz.U. 2011 nr 230 poz. 1370.

[204] Art. 2 of the Timeshare Act. See also B. Sagan, *Ustawa o timeshare. Komentarz*, LexisNexis 2014, pp. 18-25.

[205] For example services offered by Airbnb or Wimdu one of the leading online marketplaces and hospitality services covers much shorter stays.

[206] B. Gnela, *Umowa konsumencka w polskim prawie cywilnym i prywatnym międzynarodowym*, LEX Wolters Kluwer business 2013.

[207] See *inter alia* J. Paliszkiewicz, *Rola zaufania w handlu elektronicznym w świetle badań literaturowych*, in: R. Knosala (ed.), *Innowacje w Zarządzaniu i Inżynierii Produkcji*, PTZP 2015, s. 791-798; W.M. Grudzewski, I.K. Hejduk I. K., A. Sankowska, M. Wańtuchowicz, *Zarządzanie zaufaniem w organizacjach wirtualnych*, Difin 2007.

comprehensive data with cross-sector relevance[208]. Certain generalisation in formulating conclusions on trust building mechanism is thus unavoidable.

Buyers' trust could come from up-front inspection of merchandise; from sellers' reputation; from enforcement.

When a decision on sales is usually reached by only looking at the goods on the internet, the first issue is problematic. Multiple studies explore a possibility for misrepresentation and reveal a general (although not uniform) trend that online sellers tend to overstate the quality of their products. Some leading undertakings in collaborative economy business (like Airbnb) offers to have certified product description[209]. Such solutions are "internal" in nature as they solely depend on company's goodwill. Also, the question is how effective are these trust-building measures. An alternative approach is to have certain "vetting" mechanism legally imposed. Here too, the issue of effectiveness remains. Pro-consumer money back guarantee and compensation mechanism could also be considered as a complementary mechanism. It is, however, a two-edged sword, as on the one hand, it is sending a clear message that company has a serious approach towards customer service, but on the other, it could drive up the costs, and it is prone to abuses.

A key component of trust-building is feedback mechanisms. Research are showing a significant impact of these solutions which at the same time are easy to set up and run. However, its various shortcomings are also evident. The primary concern is the risk of possibly fraudulent feedbacks. Individuals may be deterred from honest reviews through the threat of retaliatory feedback. Also, the research shows that a significant number of unsatisfied customers are leaving without feedback[210]. With the development of sharing economy, business feedback mechanisms are getting increasingly sophisticated. Two-sided-reviews merits its mentioning in this regard. Some trade intermediaries (like Uber or Airbnb) offering feedback option for both parties to screen fraudulent customers[211]. The experience of Airbnb shows that when reviews can be written only after the confirmed transaction and especially when incentives for reviewing are in place

[208] L. Einav, C. Farronato, J. Levin, *Peer-to-Peer Markets*, Annual Review of Economics (8)2016, pp. 615-635.

[209] Various online platforms can introduce additional safety mechanisms such as Insurance requirements; Logged private messaging system; Secure payments (i.e. through PayPal); Security deposits; Verification of identity; Linking to social network accounts.

[210] L. Einav, C. Farronato, J. Levin, *Peer-to-Peer...*, p. 621.

[211] Conducted analysis of feedback left on TripAdvisor and Yelp website (providing reviews of travel-related content and crowd-sourced reviews about local businesses respectively) reveals very high percentage of disingenuous and manipulative reviews. See D. Mayzlin, Y. Dover, J. Chevalier J. 2014. *Promotional reviews: an empirical investigation of online review manipulation*, American Economic Review (104)2014, pp. 2421–2455.

data aggregation is better. While by no means perfect mentioned mechanisms are nevertheless probably best workable solutions. It can further be argued that well-working feedback system can to a large extent replace the need for up-front inspections.

As of enforcement, existing regulations are protecting customers against non-conformity of goods with the contract. By introducing a trust-building mechanism, the goal it to preempt litigation when possible. It is any way doubtful whether an unhappy customer of a low-value trade would go ahead with legal mechanisms. In author's opinion, it is highly doubtful whether creating sufficiently unambiguous and efficient rules for trust-building mechanisms (i.e. rating systems, certifications) is possible through hard law. Grass-roots pressure on good practices and promoting self-regulation seems to be more up to the task.

2. Digital media

Question 2.1.

At the beginning it has to be noted that Polish Broadcasting Act [*Ustawa o radiofonii i telewizji*] implementing AVMSD Directive uses term *audycja* which can be translated into English as "Broadcast", "Audition", "Programme" to describe concept enshrined in 1(1)(b) of the AVMS Directive[212]. The Same term is used in the Polish version of the AVMS Directive[213]. At the same time mentioned Broadcasting Act introduced the concept of *program*, which could also be translated as "Programme" but likewise "Telecast" or "TV Schedule" to describe a string of individual auditions (and/or commercial communications, or other communications) in a specific order that could be received simultaneously by a number of end-users[214]. For the Purpose of this analysis, the term "Programme" will be used with the meaning of 1(1)(b) of the AVMS Directive to denote *audycja* in Polish Broadcasting Act.

Polish Broadcasting Act provides broad subjective scope, but it explicitly excludes online versions of periodicals and newspapers provided its content is not "predominantly" audio-visual in nature[215]. In practice, online versions are not always identical with its printed counterparts, and there is another problematic distinction between the online version and a portal linked with given newspaper

[212] Article 4(2) of the Broadcasting Act [*Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji*], Dz.U. 1993 nr 7 poz. 34, Consolidated Version Dz. U. z 2016 r. poz. 639, 929.

[213] Definitions in Polish Broadcasting Act and the Directive are almost identical.

[214] Article 4(6) of the Broadcasting Act; J. Sobczak, *Radiofonia i telewizja. Komentarz*, Zakamycze 2001, p. 81-82.

[215] Article 2(6) of the Broadcasting Act. E. Czarny-Drożdżejko, *Nowelizacja ustawy o radiofonii i telewizji w zakresie dostosowania do dyrektywy europejskiej o audiowizualnych (wybrane aspekty)*, Przegląd Prawa Publicznego (7-8)2013. p. 35

(which often uses some variation of its name)[216]. Therefore as the concepts of "online version", and "predominant part" are ambiguous it is not entirely clear whether Broadcasting Act or Press Law is applicable[217].

In doctrine, it is emphasised that "programme" it must have stand-alone nature and be distinguishable because of its content, form or authorship[218]. According to this line of reasoning, one could deduct that if short videos in question are topic-related to the adjacent text these should be treated as a part of one programme. If on the other hand, these clips are of separated nature then it constitutes an individual programme[219]. Although there is hardly any case law on the definition of "programme". Assuming activity in question would fall under Broadcasting Act its current wording which uses adjective "audio-visual" [pol. *audiowizualna*] as a descriptor of "programme" allows for interpretation in-line with CJEU's C-347/14 *New Media Online GmbH v Bundeskommunikationssenat* ruling.

Question 2.2.

In Poland, there are no dedicated rules on publishing on the Internet [220]. Depending on the type of content either Broadcasting Act or Press Law is applicable[221]. Platforms offering on-demand video content falls under former act[222].

The original Directive (2010/13/EU) explicitly provides that it "(...) not affect the responsibility of the Member States and their authorities with regard to the organisation — including the systems of licensing, administrative authorization (...)"[223]. However to offer "audio-visual media services" [pol. *Audiowizualne usługi*

[216] It is emphasized in the doctrine that printed and e-versions must be identical in content S. Piątek (ed.), *Ustawa o radiofonii i telewizji. Komentarz*, C.H. Beck 2014, p. 26; T. Zdzikot, *Status prawny telewizji hybrydowej na gruncie przepisów ustawy o radiofonii i telewizji*, internetowy Kwartalnik Antymonopolowy i Regulacyjny (4)2015, pp. 19-28.

[217] E. Czarny-Drożdżejko, *Glosa do postanowienia Sądu Najwyższego z 26 lipca 2007 r., IV KK 174/2007,* Przegląd Prawa Publicznego (9)2008, pp. 84-88.

[218] The legal definition is contained in Article 4(6) of the Broadcasting Act. E. Czarny-Drożdzejko, *Ustawa o radiofonii ...*, p. 57-58.

[219] S. Piątek (ed.), *Ustawa o radiofonii i telewizji...*, p. 41.

[220] Specific liability regime applies only to certain hosting services not to publishing. See details in Section 1.1.

[221] This distinction is not always clear. See analysis in question 2.1. The AVMS Directive has been implemented in Poland by the following acts: Broadcasting Act; Press Law; Act on the Provision of Services by Electronic Means; Act on the Freedom of Economic Activity.

[222] Article 1a in relation with Article 4(1) of the Broadcasting Act. Additionally regulatory framework for providing online services is provided in the Telecommunication Law. Former act covers „software" sphere (content) while the latter „hardware" aspects.

[223] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audio-visual media services (Audio-visual Media Services Directive), OJ L 95, 5.4.2010, p. 1, recital 19

medialne] an entity (natural persons, legal persons, commercial-law-companies) is subjected to the registration requirement[224]. There has been quite a heated debate on this issue as it has been pointed that this could lead to potential censorship of the internet at the same time de facto introducing a licensing scheme[225]. The official position of both Polish government and regulatory body – the National Broadcasting Council is that these concerns are unfounded as there are no discretionary powers to refuse registration, apart from purely formal ones pertaining to submitting required paperwork[226]. While this is true, it remains unclear why such registration is needed in the first place.

In this context, looking at the proposition to extend the scope of AVMS directive it remains unclear what would be the cost of increased administrative burdens stemming from increased oversight. At the same time, it is hard to judge the overall effectiveness of enforcement mechanism which is always problematic in the case of internet due to the extraterritorial dimension of online services. Last but not least serious question exists of how "aggressively" regulator could pursue its policy objectives under the guise of preventing illegal content. In other words, the risk of potential censorship is ever-present. So far these questions remain unanswered.

Furthermore, the author would like to emphasise especially negative opinion about encapsulated requirement of promotion of European contents[227]. It is unreasonably intrusive intervention in the content in itself, and author sees absolutely no reason why end-users should not be unhindered in their freedom of choice[228].

In author's opinion, the openness of the Internet is the value in itself, and it should not be subjected to heavy-handed regulation. Having said that it could not be overlooked that there are certainly unwanted phenomena on the internet like hate speech, racism, and so forth. None the less discussed proposal raises

[224] Although in common language this notion refers to Video on demand (display) (VOD), the legal term „audio-visual media services" have wider scope as it cover both on demand and scheduled services, so the registration requirement was not introduced with the exclusive aim at on demand services.

[225] Such opinion was especially prevalent among NGOs monitoring freedom of speech.

[226] Official communique including point to point rebuttal of critique is available on the National Broadcasting Council's website at: http://www.krrit.gov.pl/krrit/aktualnosci/news,437,informacja-krrit-dotyczaca-implementacji-dyrektywy-o-audiowizualnych-uslugach-medialnych.html (11.05.2017).

[227] Article 13 of the draft AVMS Directive. Text available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1464618463840&uri=COM:2016:287:FIN (12.05.2017).

[228] Additionally it can be argued that such provision is infringing Article 54 of the Constitution of Poland ([*Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r.*], Dz.U. 1997 nr 78 poz. 483) guaranteeing freedom of speech especially given that recital 39 of the draft AVMS Directive explicitly states that the Directive recognizes fundamental rights.

significant questions if it comes to its consequences. it stands to reason that policymaking requires extensive cost-benefit analysis. Increasing administrative burdens on undertakings should in principle be judged negatively and accepted only if there is a clear-cut overriding goal.

Question 2.3.

The mentioned problem was recognised by the National Broadcasting Council in its opinion to the proposed amendment of the original audio-visual Directive 2010/13[229]. The Council expressed the view that although envisaged changes are to be welcomed in principle they are not sufficient. It was pointed out that enforcement is lacking especially cooperation mechanisms between national regulators issuing so-called "de-localised" licenses[230]. As a result, the Council concluded, there is a double standard of treatment of operators offering services in the domestic market (targeting national audience).

Currently, Polish lawmakers introduced mechanism aimed at preventing "jurisdiction shopping" fashioned after solutions contained in Directive 2010/13[231]. Anti de-localisation instrument encapsulated in the Articles 46a and Article 46b of the Broadcasting Act [pol. *Ustawa o radiofonii i telewizji*] consist of three components:

First introduces consultation procedure with the Member State where broadcaster, allegedly offending Polish law is located, and with the European Commission[232]. If within two months from the start of consultation procedure broadcaster do not cease transmitting offending content, the programme in question is delisted from the registry[233]. In principle every program broadcasted through teleinformatic network [pol. *sieć teleinformatyczna*] falls under registration requirement[234]. Registration in itself is purely technical act and it's not subject to any discretionary powers of the registering authority, therefore, it cannot be

[229] National Broadcasting Council's official position entitled *Uwagi KRRiT do projektu nowelizacji Dyrektywy 2010/13/UE o audiowizualnych usługach medialnych* is available at: www.prawoautorskie.gov.pl%2Fmedia%2Fkonsultacje_Dyrektywa_audiowizualna%2FKRRiT.docx (27.05.2017).

[230] K. Chałubińska-Jentkiewicz, *Audiowizualne usługi medialne, Reglamentacja w warunkach konwersji cyfrowej*, LEX Wolters Kluwer 2013, p. 286.

[231] The term „jurisdiction shopping" (alternatively called „forum shopping") refers to the practice adopted by some litigants of having their legal case lodged in the jurisdiction containing most favourable provisions.

[232] E. Czarny-Drożdzejko, *Ustawa o radiofonii i...*, p. 457.

[233] Article 46b(4) of the Broadcasting Act. E. Czarny-Drożdzejko, *Ustawa o radiofonii i...*, p. 458-459. It should be noted in this context that Broadcasting Act contain no procedure for temporary suspension of allegedly offending content in-line with the European Convention on Transfrontier Television, Dz.U. 1995 nr 32 poz. 160.

[234] Article 41 of the Broadcasting Act.

regarded as a form of licence[235]. Consequences for operating without registration are twofold: First a person responsible – representative of a broadcaster – could be held personally liable for failure to follow registration requirement[236]. Secondly, the broadcaster – an undertaking – could be fined[237]. From the broadcaster's standpoint transmitting without a valid registration is not a criminal offence in itself (unlike broadcasting without a license when it is required) and therefore it is unlikely that an audition could be suspended on this basis. Although in theory the operator can be fined on a continuous basis (however interval remains unknown). The regulation is not entirely clear on this point, but in the case of off-country undertakings, these measures are not especially dissuasive given predictable problems with enforcement[238].

Secondly, if provider located outside Poland (but within the EU) is targeting domestic audience with all or majority of its program [pol. *w przeważającej części*], the Council's Chairman, could request from Member State where this operator is located to enact "appropriate measures" [pol. *odpowiednie rozwiązania*] aimed at safeguarding public interest rules encapsulated in Broadcasting Law, and other specific provisions of Polish law[239]. If within two months from request mentioned "appropriate measures" had not been enacted Poland can notify the European Commission about given State's inaction in preventing circumvention of Polish broadcasting provisions by undertaking located in its territory[240]. In this case, National Broadcasting Council is also announcing an intention to unilaterally impose measures of removing offending provider's programme from a list of licenced auditions or enacting other measures provided these be non-discriminatory and proportional.

Finally, these mentioned unilateral measures can be enacted but only upon receiving a go-ahead from the European Commission[241]. The EC within three

[235] In Polish doctrine such acts are called „material-technical activity" [pol. *czynność materialno techniczna*] – an actual acts that have a legal basis and have legal ramifications. See M. Wierzbowski (ed.), *Prawo Administracyjne, Wydanie 9*, LexisNexis 2009, 295-296.

[236] Article 52(2) of the Broadcasting Act. It is considered a criminal misdemeanour. Rules encapsulated in the Criminal Code apply accordingly.

[237] Article 53a of the Broadcasting Act. Fine could reach a ceiling of 10% of broadcaster's annual income from the previous year.

[238] E. Czarny-Drożdzejko, *Ustawa o radiofonii i...*, pp. 456-459.

[239] K. Chałubińska-Jentkiewicz, *Audiowizualne usługi...*, p. s. 291. Whether allegedly offending content is targeted at audience in other State is established on the basis of programmes' language, assessment from which country majority of operator's revenues come from, and of analysis whether programme content has specific characteristics that are clearly designed for audience in a given country (i.e.,. covers contemporary issues of that country, or advertises goods that can be purchased specifically in a particular State).

[240] K. Chałubińska-Jentkiewicz, *Audiowizualne usługi...*, p. s. 292.

[241] Article 46a(2)2 of the Broadcasting Act.

months from State's request will assess whether proposed measures are in line with the EU law. The measures in question may include a removal from the registry, refusal to register, or other proportional and nondiscriminatory measures.

Additional serious problem with the abovementioned mechanism and generally with applying domestic rules to off-country providers lies with the vagueness of Article 18 of the Broadcasting Act which contains set of standards required for all broadcasted programmes. The provision refers to non-definable (at least in legal terms) concepts as "morality" or "Christian values". It is widely accepted both in jurisprudence and in the doctrine that the article in question consists general clauses allowing limiting freedom of speech, and therefore must be applied with special prudence[242]. Over the years there has been many cases here National Broadcasting Council was accused of being overzealous in its attempts to police the media while being overly lenient for certain other viewpoints.

It then stands to reason that regardless of how the streamlined, and well-designed procedure is going to be the mechanism will always be burdened by the lack of legal certainty if the material law provision that triggers it remains ambiguous. At the same time, such vagueness is inevitable whenever the application of law boils down to an axiological value judgment as in the case of Article 18 of the Broadcasting Act. So far in Poland, there has been no attempts to block foreign programmes targeted at national audience similar to Mesopotamia Broadcast/Roj TV case[243]. However, this is not due to an inactivity of national regulators but rather that there are no overtly unlawful programmes.

Question 2.4.

Regulator's independence is something that should be strongly endorsed. There is a vast body of research works dedicated to role, functions, and benefits of independent regulators in a market economy[244]. It is widely accepted that regulation a key tool for achieving the social, economic and environmental policy objectives of governments[245].

[242] S. Piątek, *Ustawa o radiofonii i telewizji...*, p. 52

[243] Analysis of this case lies beyond the scope of this report. Details are available in the CJEU's Joined Cases C-244/10 and C-245/10 *Mesopotamia Broadcast A/S METV and Roj TV A/S v Bundesrepublik Deutschland*, ECLI:EU:C:2011:607.

[244] See *inter alia* M. Swora, *Niezależne organy administracji*, PWE 2012; M. Szydło, *Prawo konkurencji a regulacja sektorowa*, Wolters Kluwer business 2010; M. Szydło, *Krajowy parlament jako regulator sektorów sieciowych* LEX Wolters Kluwer business 2013; T. Bąkowski, *Organizacja administracji publicznej z perspektywy powierzanych jej zadań*, LEX Wolters Kluwer business 2015; T. Skoczny (ed), *Prawo Konkurencji...*

[245] In specific context of audio visual media see *inter alia*: I. Kawka, *Telekomunikacyjne organy regulacyjne w Unii Europejskiej*, Zakamycze 2006; K. Chałubińska-Jentkiewicz, *Media audiowizualne. Konflikt regulacyjny w dobie cywilizacji*, LEX Wolters Kluwer business 2011; M. Rogalski (ed.), *Prawo Telekomunikacyjne*, LEX Wolters Kluwer business 2011; A. Monarcha-Matlak *Obowiązki administracji w komunikacji elektronicznej*,

In Poland, there is a peculiar regulatory setup of audiovisual media with partially overlapping competences between National Broadcasting Council and Office of Electronic Communications[246]. In principle, the former institution should focus on "software" (content) aspects while the latter limit itself to the "hardware" (technical) sphere[247].

Since its inception, the Council has been given prominent legal status – its core powers are regulated directly by the Constitution (specific competencies, procedures, etc. are regulated by the Broadcasting Act)[248]. There is ongoing controversy as to what is the legal status of this body and on the scope of its mission statement[249].

Article 213(1) of the Constitution stipulates that the Council „Stands guard over freedom of speech, right to information, and public interest in radio and television[250]. Article 6(1) of the Broadcasting Act offers more guidance as states that the Council aims to achieve "independence of media services, protect the interest of end-users, achieve open and plural nature of radio and television"[251].

Wolters Kluwer, 2008; H. Babis, K. Flaga-Gieruszyńska (eds.), *Rynek usług telekomunikacyjnych*, LEX Wolters Kluwer business 2011; E. Galewska, *Obowiązek zawarcia umowy o połączeniu sieci telekomunikacyjnych*, LEX Wolters Kluwer business 2015; K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, LEX Wolters Kluwer business 2015.

246 In Administrative Law doctrine there is a distinction between „*Office*" [pol. *urząd*] and „*Organ*" [pol. *organ*]. The former denotes a certain administrative structure that allows a performance of given tasks. The latter denotes a basic building block of an administrative system equipped with specific competences. In a nutshell office is subordinated to an organ and form its organizational backbone. These terms are thus interlinked although not synonymous in a legal sense. This report takes a functional approach and looking at a given administrative body, mentioned distinction will be omitted. See further J. Boć, *Pojęcie organu. Pojęcie urzędu*, in: J. Boć (ed.), *Administracja publiczna*, Kolonia Limited 2003, pp. 156, 172-173.

247 Articles 5-12 of the Broadcasting Act. E. Czarny-Drożdzejko, *Ustawa o radiofonii i ...*, p. 89-90; J. Sobczak, *Radiofonia i telewizja. Komentarz*, Zakamycze 2001, p. 107 et seq.; K. Chałubińska-Jentkiewicz, *Audiowizualne usługi medialne...*, pp. 143-144.

248 W. Lis, *Status Prawny Krajowej Rady Radiofonii i Telewizji*, Roczniki Nauk Prawnych XXV(3)2015; pp. 158-159. H. Zięba-Załucka, *Krajowa Rada Radiofonii i Telewizji a regulatory mediów w państwach*, Wydawnictwo Uniwersytetu Rzeszowskiego 2007, p. 199.

249 J. Boć (ed.), *Konstytucje Rzeczypospolitej oraz komentarz do Konstytucji RP z 1997 roku*, C.H. Beck 1998, p. 315; K.A. Wąsowski, *Status prawny Krajowej Rady Radiofonii i Telewizji – próba charakterystyki*, Kwartalnik Prawa Publicznego (1)2004, pp. 223; B. Szmulik, K. Miaskowska-Daszkiewicz, *Administracja publiczna. Ustrój administracji państwowej centralnej, t. I,* , C.H. Beck 2012, p. 249 et seq.; R. Chruśniak, *Krajowa Rada Radiofonii i Telewizji w systemie politycznym i konstytucyjnym*, Elipsa 2007.

250 See L. Garlicki (ed.) *Konstytucja Rzeczypospolitej Polskiej. Komentarz, t. III,* Wydawnictwo Sejmowe 2003, p. 9; M. Haczkowska (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, LexisNexis 2014, pp. 546-549; L. Garlicki (ed.) *Konstytucja Rzeczypospolitej...*, p. 10. See also analysis A. Bodnar, A. Gliszczyńska-Grabias, R. Wieruszewski, M. Wyrzykowski (eds.), *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*], Wolters Kluwer 2010.

251 K. Chałubińska-Jentkiewicz, *Media audiowizualne...*, pp 248-249.

The terms "radio and television" is interpreted broadly as audiovisual services thus it is widely accepted that the Council could regulate certain internet activities provided these not fall under Press Law[252].

Although National Broadcasting Council is autonomous, it is not impartial. The Council consists of five members appointed for a six years term: two by the Lower Chamber of the Parliament, one by the President, and one by the Upper Chamber of the Parliament[253]. While appointing body cannot dismiss Council member the fact that it consists of political nominees' weights heavy on its independence[254]. The lack of impartiality raised especially significant controversies in the 90's. The primary problem back there had related to frequency allocation in the emerging TV and radio market[255]. With the emergence of digital broadcasting the issue lost most of its prominence, but nevertheless, complaints about Council's insufficient oversight over media activities (i.e. in combating hate speech, racism) are ever-prevalent[256]. Sometimes the body in question is also accused of attempts of censorship under the guise of protecting, among others, Christian values or national symbols[257].

The scope of National Broadcasting Council's competencies inevitably brings it into competence conflict with the Office of Electronic Communications which is yet another regulatory body[258]. Although the Office is described as "regulator",

[252] See question 2.1. See also W. Skrzydło (ed.), *Polskie Prawo Konstytucyjne*, Lubelskie Towarzystwo Naukowe 1998, p. 448 where authors expressed view that scope of the Council's oversight should be limited to public media (State owned), because Article 213 of the Constitution uses the term "public interest". This approach was widely criticized in doctrine (*inter alia* E. Czarny-Drożdzejko, *Ustawa o radiofonii* ..., pp. 91-94; J. Sobczak, *Radiofonia i telewizja*..., pp. 112-114) and there are no doubts that all media are within the scope of Council's oversight.

[253] Article 214 of the Constitution. The Constitution do not regulate Council's specific composition, only stating which institutions are competent to appoint its members. Specific rules are provided by Article 7 of the Broadcasting Act.

[254] The issue attracted significant media attention. Also see *inter alia* analysis W. Brzozowski, *Bezstronność światopoglądowa władz publicznych w Konstytucji RP*, Wolters Kluwer business 2010, pp. 154 et seq.

[255] See *inter alia* D. Waniek, *Dylematy ładu medialnego RP: standardy europejskie a praktyka*, KTE 2007.

[256] See *inter alia* A. Bodnar, A. Gliszczyńska-Grabias, R. Wieruszewski, M. Wyrzykowski (eds.), *Mowa nienawiści a*...; W. Brzozowski, *Bezstronność światopoglądowa władz*...; D. Waniek, *Dylematy ładu medialnego*....

[257] Case of the artist Marek Raczkowski provides especially instructive illustration of the controversies the issue stirs. In 2008 Mr Raczkowski during TV program had stuck little Polish flags in dummy dog's faeces to point out the problem of not cleaning after pet animals. While the taste of this performance or happening could be discussed, sticking to the legal question, the National Broadcasting Council fined the TV station for „offending values common to all member s of society" (the Council pointed at infringement of Article 137 of the Criminal Code which protects national symbols). The fine was upheld in courts including the Supreme Court who claimed that „broadcaster is bound by the constitutional and legal obligation to respect national symbols" (case III SK 42/12). The case was in the media spotlight and raises a profound questions where is the „thin red line" between the need of protecting certain value and censorship.

[258] K. Chałubińska-Jentkiewicz, *Media audiowizualne*..., pp. 259-260. Additionally it can be argued that there is certain overlap with the competences of Office of Competition and Customers Protection.

its tasks include protecting competition by *inter alia* combating abuses of dominant position and overseeing public service obligations[259]. It could be argued that Council is entirely redundant if the Office could act as *par excellence* regulator, but the former institution is "anchored" in Constitution, so its interference seems inevitable[260]. For the sake of discussion one could (speculatively) consider dismantling the Office and moving its non-overlapping competencies to the Council (which is much easier from the legislative standpoint), but then the regulator will not remain impartial. The legal framework of the Office is described in detail in question 3.4.

To conclude, the regulatory setup requires a major overhaul, but it could only be done through amendment of Constitution as general provisions on its composition and members' appointment of the National Broadcasting Council are contained there. So far there was no political impetus in Poland to establish cohesive, and impartial regulatory order for audio-visual activities, therefore "external" pressure from the AVMS Directive is to be welcomed.

Question 2.5.

In author's opinion, the most contentious issue of the media environment in Poland is the functioning of public media, especially public TV[261]. Following specific points are of relevance:

Political impartiality: Existing mechanisms designed to safeguard objectivity of presented information, and political impartiality are woefully inadequate. Because of politicisation of TV management, public media are regarded as "Political Loot", and after elections winning political option is usually taking control over both Radio and especially TV. This problem exists since the change of political system, and despite numerous attempts to change the corporate governance of public media, nothing has been done. The insufficient regulatory oversight further exacerbates the problem[262].

[259] The Office for Electronic Communications is acting under Telecommunication law.

[260] See *inter alia* K. Chałubińska-Jentkiewicz, *Media audiowizualne...*, pp. 260-262; K. Chałubińska-Jentkiewicz, *Problematyka kwalifikacji prawnej usług telewizji komórkowej DVB-H*, Przegląd Prawa Handlowego (7)2008, pp. 33-38

[261] Public (State owned) media in Poland consist of following TV stations: TVP1, TVP1 HD, TVP2, TVP2 HD, TVP3 (regional stations in Białystok, Bydgoszcz, Gdańsk, Gorzów Wielkopolski, Katowice, Kielce, Kraków, Lublin, Łódź, Olsztyn, Opole, Poznań, Rzeszów, Szczecin, Warszawa, Wrocław), TVP Polonia, TVP Info, TVP Info HD, TVP Sport, TVP Sport HD, TVP Historia, TVP Kultura, TVP HD, TVP Parlament, TVP Seriale, TVP Rozrywka, TVP ABC, Belsat (channel in Belorussian language). Additionally there radio operator Polskie Radio consisting of four main stations and seventeen regional stations independent of main broadcaster. These undertakings are explicitly listed as "public broadcasters" [pol. *nadawca publiczny*], and tasked to discharge public service obligation as per Article 26 and 30 in relation to Article 64 of the Broadcasting Act.

[262] W. Brzozowski, *Bezstronność światopoglądowa władz publicznych w Konstytucji RP*, Wolters Kluwer 2010; D. Waniek, *Dylematy ładu medialnego ....*

Financing mechanism: Under existing regulations every media entrusted in discharging public service obligation [pol. *realizacja misji publicznej*] are entitled to revenues from Radio and Television Licence[263]. The National Broadcasting Council sets the distribution algorithm[264]. In theory, every natural person (with some exceptions) who owns TV and radio for his/her personal use is required to register this set and pay a licence fee on a monthly basis[265]. In practice, these requirements remain a dead letter. According to National Broadcasting Council hardly anyone is registering their hardware, and licence fee's collection rate oscillates between ten and thirty percent[266]. Nevertheless, revenue from this source is noticeable from the public broadcaster's standpoint[267]. In turn, it create a competition issue as public media are also allowed to profit from advertisements. The first controversy relates to potential cost advantage stemming from additional revenues[268]. Secondly, public media are often being accused of using dumping prices for broadcasting advertisements with obvious detriment for non-public competitors. These controversies exist mainly because there is a real competition between public media and private media enterprises which lead to the third contentious issue described below.

Programme content: In principle, public media should primarily focus on discharging public service obligation (which is *raison d'être* of Licence fee), and

[263] Discharging public service obligation as stipulated in Article 21(1) of the Broadcasting Act is financed by the mandatory license fees regulated by the Act on License Fees [*ustawa z dnia 21 kwietnia 2005 roku o opłatach abonamentowych*], Dz.U. z 2005 roku Nr 85, poz. 728 i Nr 157, poz. 1314.

[264] Article 8 of the Act on License Fees.

[265] Article 4 of the Act on License Fees contain list of categories of persons exempted from this obligation. An Individual is required to submit declaration proving his/her eligibility for exemption which is problematic in practice as most people are not aware of this. See judgment of Voivodship Administrative Court in Gliwice in case 07.06.2016, I SA/Gl 669/15, where Court held that the mere fact of being qualified for exemption is not a sufficient basis for ceasing payments, and it is necessary to complete the required formalities. Similar reasoning in judgment of Voivodship Administrative Court in Szczecin, 19.07.2016, I SA/Sz 604/16, where court held that exemption on the basis of reaching age of 75 is only applicable if a person submits relevant declaration with documents proving entitlement for exemption. See also M. Panek, P*rzesłanka wieku 75 lat jako okoliczność zwalniająca z obowiązku uiszczania opłaty abonamentowej*, Przegląd Prawa Publicznego (2)2017, pp. 63-72.

[266] Post Office is legally responsible of License fee's collection. See analyses M. Pawłowska, *Analiza prawna przepisów dotyczących ściągalności abonamentu radiowo-telewizyjnego*, Doradca Podatkowy (3)2012, pp. 39-42; E. Żelasko-Makowska, *Wpływ sankcji prawnych bądź ich braku na przestrzeganie obowiązków ustawowych przez obywateli. Studium przypadku*, Przegląd Prawa Publicznego (7-8)2015, pp. 73-84. There is ongoing debate on the reform of collection system. There are plans to include License fee in personal income tax, and to involve Revenue Services in collection enforcement.

[267] In 2016 downward trend observable in recent years somewhat stabilized. In 2016 approximately 750 million PLN was collected from 1,2 million households out of total 3,2 million required to pay. Of this Public TV received 365,5 million PLN; Public radio – 185,9 million PLN; Regional broadcasters – 170,6 million PLN.

[268] K. Chałubińska-Jentkiewicz, *Audiowizualne usługi* ..., pp. 277-278.

competition with other media enterprises should be of secondary concern[269]. In reality, the concept of "public mission" is so nebulous, superfluous and vague that it is virtually impossible to establish what kind of content fall under it (with the exception of some rare borderline cases)[270]. There are ongoing controversies whether a particular programme of public TV telecast fits "public service" role[271]. Similarly, many popular science programmes offered by non-public network stations could easily be considered as being of "public service" nature[272]. If so then one may ask, why these stations are not getting revenues from licence fee. This problem is inseparable from discussed issue of financing mechanism. Since revenues from licence fee are inadequate for covering operating costs (which at the same time are too high – company is inefficient with bloated employment), TV is forced to introduce more "marketlike" content, because only these can attract advertisers to supplement its income[273].

Currently, the situation of public media in Poland is in deadlock even though a precise diagnosis of multiple problems is well known. However, at the same time harmonisation is not an answer to every media-related problem. In this case, one will have to consider consequences of possible encroachment over national tax systems and the principle of respect for national diversity enshrined in Article 167 TFEU[274]. Therefore current quagmire of public media in Poland can only be sorted out internally, but chances for this to happen are next to none.

Question 2.6.

In Polish Law "personal data" [pol. *dane osobowe*] is defined as "any information relating to identified or identifiable natural person"[275]. Legislator deliberately constructed a wide, open-ended notion that offers maximum interpretative fle-

[269] See in this respect: K. Chałubińska-Jentkiewicz, *Misja publiczna w działalności audiowizualnej w dobie cyfryzacji – przedmiot finansowania publicznego i kierunki rozwojowe*, Przegląd Prawa Handlowego (2)2009, pp. 44-52.

[270] „Public mission" is defined in Article 21 of the Broadcasting Act.

[271] Especially if a programme is a licence version of foreign entertainment programme where in its original form is broadcasted purely commercially. he argument then run that if a given content is broadcasted in other country without any recourse to public service obligation why the same content be considered as a part of „public mission" in Poland.

[272] There was a debate whether a private (non-State owned), but purely information TV station could successfully apply for a „public broadcaster" status. In theory probably yes, but there is no existing precedent.

[273] K. Chałubińska-Jentkiewicz, *Misja publiczna w...*, pp. 45-52.

[274] See further K. Chałubińska-Jentkiewicz, *Media audiowizualne. Konflikt regulacyjny w dobie cywilizacji*, LEX Wolters Kluwer business 2011, pp. 81 et seq.

[275] Definition is provided in the Article 6 of the Personal Data Protection Act [*Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*], Dz.U. 1997 nr 133 poz. 883 ze zm.

xibility and avoiding lacunae[276]. However, some doubts remain whether browsing history, IP address would fall under this definition as it can be argued that this information can be used to identify an access point but not necessarily a specific individual using a computer at a given time[277]. Such identification will be possible upon login or if there are some other forms of password protected systems. So the first problem if it comes to data protection is a certain ambiguity whether data typically used for tailor-made advertisement falls within generic Data Protection Act[278]. Telecommunication Law [pol. *Prawo telekomunikacyjne*] contains *lex specialis* specifically to remedy this potential lacuna.

Telecommunications Law provides generic rules for targeted/personalised advertisement in all audiovisual media.[279]. Article 173 of this Act was amended to implement Directive 2002/58/EC, and Directive 2009/136/EC and thus is primarily designed to regulate the usage of "cookies" on the Internet[280]. There are no dedicated regulations of targeted or personalised advertisement in TV. Although the provision in question refers only to "End Device" so [pol. *urządzenie końcowe*] where temporary files allowing for personalised/targeted content are to be installed, so TV (and also for instance gaming console) lies within its scope[281].

[276] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz, wyd. VI*, LEX Wolters Kluwer business 2015, pp. 303 et seq.; A. Harla, *Termin „dane osobowe" – uwagi de lege lata i de lege ferenda na gruncie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, Palestra (1)2001, p. 38; G. Szpor, *Pojęcie informacji a zakres danych osobowych*, in: P. Fajgielski (ed.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, KUL 2008, p. 8.

[277] It is emphasises for a data to be „personal" in the meaning of Personal Data Protection Act, it must allow identification of a given individual which is not always the case with IP address. However CJEU in case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland* (ECLI:EU:C:2016:779) falls under the definition of „Personal Data". In the same vein the website of Inspector General for the Protection of Personal Data [pol. *Generalny Inspektor Ochrony Danych Osobowych* – GIODO] contain a communique providing basic guidance as to when IP address would be considered as Personal data (available at: http://www.giodo.gov.pl/319/id_art/2258/j/pl/ (18.05.2017)). Similar line of reasoning is also visible in case-law of Polish courts. See *inter alia* Judgment of the Voivodship Administrative Court in Warsaw [pol. *Wojewódzki Sąd Administracyjny*], 03.02.2010, II SA/Wa 1598/09; of the Supreme Administrative Court [pol. *Naczelny Sąd Administracyjny*], 21.08.2013, I OSK 1666/12.

[278] This controversy has been explicitly recognised by the Inspector General for the Protection of Personal Data in its opinion submitted to the European Commission's Article 29 Working Party. Text of the opinion *Opinia 2/2010 w sprawie internetowych reklam behawioralnych*, 00909/10/PL WP 171 is available at: www.giodo.gov.pl/plik/id_p/1935/j/pl/ (18.05.2017.

[279] The definition and scope of the notion of „advertisement" [pol. *reklama*] can only be constructed on the basis of Courts' case-law and doctrine's *acquis*. It is generally accepted that it is an information aimed at influencing customer's purchasing decision – to encourage/induce customer to buy this particular product or service (Judgment of the Supreme Court, 26.01.2006, V CSK 83/05; of the Court of Appeal in Poznań, 10.10.2005, I ACa 221/05).

[280] J.A. Krasuski, *Prawo telekomunikacyjne. Komentarz, wyd. IV*, Wolters Kluwer 2015, pp. 1350-1353.

[281] End devices are defined in Article 2(43) of the Telecommunication Law. It will primarily apply to TV decoders (or similar devices) technically capable of temporarily saving cookies. D. Karwala, *Nowe zasady*

Under existing regulations data for the purpose of tailored marketing could be collected only upon explicit consent from an individual[282]. Agreement to use "cookies" cannot be implied[283]. There is no need for a specific form (like written or electronic,), although consent must be explicit, clear and once given must be saved by the service provider for future reference[284]. Additionally, consent could be withdrawn at any time without reason given. The opt-out procedure is not described in Telecommunication law, but the act requires it to be "simple and free of charge"[285]. Analogous generic mechanism requiring clear and precise consent exists in Data Protection Act[286]. Therefore analysis in this chapter remains equally relevant for personalised advertising in all means of electronic communication not only television.

To sum up, the requirement of clear display of information about data collection for the purpose of providing personalised commercials with the possibility to opt-out is sufficient in principle. Especially if generic rules for processing of personal data are supplemented with the specific mechanism in Telecommunication Law aimed at processing information that is unlikely to be considered "personal" but is used in targeted advertising. There doesn't seem to be any unique characteristic of television warranting the introduction of specially tailored solutions.

Question 2.7.

Article 10 of the Directive 93/83/EEC which provides an exemption to generic rules rules was only implemented in 2016[287]. Amendment plans were met with stiff resistance from copyright management organisations[288]. Their argument ran that new rules will deprive authors of their due profits because proposed

przechowywania informacji w telekomunikacyjnych urządzeniach końcowych (uwagi na temat z znowelizowanego art. 173 Prtelekom), Monitor Prawniczy (8)2013, pp. 15-21; S. Piątek, *Prawne warunki stosowania Cookies*, Internetowy kwartalnik Antymonopolowy i Regulacyjny (4)2015. pp. 49-2.

[282] Article 174 of the Telecommunication Law.

[283] J.A. Krasuski, *Prawo telekomunikacyjne...*, pp. 1352.

[284] S. Piątek, *Prawne warunki stosowania...*, pp. 62-66.

[285] Article 174 of the Telecommunication Law.

[286] Article 7(5) of the Personal Data Protection Act. T. Szewc, *Zgoda na przetwarzanie danych osobowych*, Państwo i Prawo (2)2003, pp. 87-96; M. Krzysztofek, *Zmiana przepisów o zgodzie na przetwarzanie danych osobowych*, Przegląd Prawa Handlowego (4)2011, pp. 57-58.

[287] Directive was implemented through the Act of July 25th 2003 on the Amendment of the Copyright Law [Ustawa z dnia 25 lipca 2003 r. o zmianie ustawy o prawie autorskim i prawach pokrewnych], Dz.U. 2003 nr 166 poz. 1610, and Amendment was introduced by *Ustawa z dnia 19 lipca 2016 r. o zmianie ustawy o prawie autorskim i prawach pokrewnych*, Dz.U. 2016 poz. 1333.

[288] The initiative was protested by ZAiKS (Polish Society of Authors and Composers), ZASP (Polish Actors Association), STOART (Artists Association STOART), SAWP (Association of Artists Performers of Musical and Vocal and Musical Works) and SFP (Association of Polish Filmmakers).

changes goes beyond of what is required by the directive[289]. It is true that initial draft did not refer to "own transmissions" [pol. *własnych transmisji*] – "home production" in other words – but the transmissions in general which raised some concerns as a possible enlargement of the exemption's scope, but final version literally repeated wording of the directive[290].

Nevertheless, copyright management organisations claimed that the exemption effectively abolishes the general rule according to which all copyright must be handled by dedicated organization, contending that in essence every initially broadcasted content is "own"[291]. Critics further claimed that regime of facultative individual license agreements is unrealistic in practice as there is no way to monitor whether an individual agreement exists for a vast number of works[292]. Moreover, it was argued that amendment is not properly coordinated with the concurrently run effort to implement Directive 2014/26/EU and that these two acts partially overlap[293]. Finally, it was rightly pointed that Polish legislator took action thirteen years after the implementation deadline[294].

On this point, it is glaringly obvious that the delay is inexcusable. However, this does not mean that the exemption is outdated in itself nor its *ratio legis* invalid. Such view was vehemently upheld by the associations of providers/broadcasters. These organisations took generally favourable view of the amendment claiming that it will help to dismantle *de facto* monopoly of certain copyright management organisations. Organisations that, according to this position, grew complacent, and fails in their primary mission. Furthermore, it was contended that by granting the artists the freedomee to self-manage their copyright and choose managing body should they wish so, will introduce competition into collective management[295].

[289] Joint petition of ZASP, STOART, and SAWP sent to Minister of Culture and National heritage – constitutionally responsible for this sphere – where these organizations outline their position on mentioned amendment is available at the website of Government Legislation Centre [pol. *Rządowe Centrum Legislacyjne*] at: https://legislacja.rcl.gov.pl/docs/2/12280160/12329049/12329052/dokument213280.pdf (01.05.2017).

[290] The amending act added Article $21^1(1^1)$ to the Copyright law.

[291] Joint petition, p. 2.

[292] *Ibidem*., p. 3.

[293] As of 01.05.2017 the Directive has not been implemented into Polish Legal order. Draft of law on collective management of copyright and related rights [pol. *Projekt ustawy o zbiorowym zarządzaniu prawami autorskimi i prawami pokrewnymi*] is currently under consultation procedure. Text is available at the Government legislation Centre at https://legislacja.rcl.gov.pl/projekt/12297411 (01.05.2017).

[294] Joint petition, p. 4.

[295] Positive opinion expressed by *inter alia* Konfederacja „Lewiatan" (an employers' organization). Organization's opinion to amendment is available at the Government Legislation Centre's website at: https://legislacja.rcl.gov.pl/docs//2/12280160/12329049/12329052/dokument207957.pdf (01.05.2017).

By looking at the validity of collective management organisations' claims the opposite seems to be true in light of growing prominence of Creative Commons and generally speaking Open Source licenses. These are not contrary to the very principle of collective copyright management, but almost inevitably frictions emerge with well-established copyright organisations[296]. Only the 2016 amendment which implements mentioned exemption changes this situation. It cannot be quantifiably attributed to these legislative changes, but the fact remains that Creative Commons and open source distribution are steadily gaining popularity. In turn, it requires an update of the rigid regime for copyright licensing.

Question 2.8.

Arguably the most severe legal barrier is the territorial delimitation of licence agreements. Article 66 of the Copyright Law contain so-called territoriality principle [pol. *zasada terytorialności*] where it stipulates that licence agreement entitling to the use of the work in question for a period of five years on the territory of the State where it had been issued[297]. Currently, it remains unclear how to establish licensee's place of residence[298]. It could be argued that generic rules from the Civil Code under which location of residence for every individual is the place where this person "resides with the intention of permanent stay" is applicable[299]. It would be the case if the place of residence is established under Polish law but mentioned Article 66 of the Copyright law provides no conflict rule for international jurisdiction (and thus can't be regarded as private international law provision)[300]. So the rules of Copyright Law and Civil Code could be used if the place of residence is in Poland. But if it is abroad, it seems that interpretation *per analogiam* with the rule from Article 59 of the Regulation 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters could be used. This article stipulates that to determine whether the party is domiciled in another Member State, the court shall apply the law of that Member State[301]. It provides a workable way around, but it is not entirely clear whether such inference is acceptable here[302].

[296] A. Jastrzębska, *Organizacje zbiorowego zarządzania prawami autorskimi a Creative Commons*, Zeszyty Naukowe Uniwersytetu Jagiellońskiego (2)2010, pp. 20-33.

[297] Article 66 of the Copyright Law.

[298] D. Flisak (ed.), *Prawo autorskie i ...*, pp. 898.

[299] J. Barta, R. Markiewicz (eds.), *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, wydanie*, LEX Wolters Kluwer business 2011, p. 415.

[300] D. Flisak (ed.), *Prawo autorskie i prawa pokrewne. Komentarz*, LEX Wolters Kluwer business 2015, pp. 898.

[301] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 012 , 16.01.2001 p. 1.

[302] Application of *per analogiam* reasoning is limited and somewhat controversial. See *inter alia* B. Brożek, *Rationality And Discourse*, Oficyna Wolters Kluwer, Warszawa 2007.

In an official position on Communication *A Digital Single Market Strategy for Europe*, the Polish Government (prepared by Ministry of Administration and Digitalisation) expressed the view that territoriality principle allows for customisation of content to reflect country specificity and particular customers' needs[303]. The document points that uneven transposition (document did not elaborate what precisely does it mean) of European legislation on intellectual property rights serves as a barrier to the cross-border portability of digital content[304].

It is hard to answer the second part of the question without a detailed cost analysis. The problem lies with the blurry distinction between "permanent" and "temporary" residence, so there is no guarantee that even regular checks be effective. In author's opinion, the latter part of mentioned question boils down to a policy choice of striking a balance between the extent of portability and the acceptable margin of abuses.

3. Digital infrastructures

Question 3.1.

In 2006 the President of the Office of Electronic Communications issued a decision concerning neutrality of transmission services between various telecommunication operators[305]. The decision had entrusted now defunct monopolist Telekomunikacja Polska S.A. (TP S.A. – former public network operator) with the obligation of equal treatment for all operators utilising its network[306]. The general requirement for such equal access, closely resembling "Essential Facilities Doctrine" from the EU law, had initially been provided by the Article 36 of the Telecommunication Law covered transmission of internet protocol suites, between TP S.A. subscribers and third party's customers[307]. The initial approach to net neutrality was focused on preventing abuses of dominant position by the network operator especially by degrading service quality for competitors using their network[308].

[303] Government Position is available at: http://m.mc.gov.pl/files/stanowisko_rzadu_do_komunikatu_ke_ws._strategii_jednolitego_rynku_cyfrowego_1.pdf (17.05.2017).

[304] Government Position, p. 7

[305] Decision of 10.06.2006, DRT-SMP-6072-1/05 (37).

[306] Telekomunikacja Polska S.A. was established in 1991 as publicly listed company wholly owned by the State Treasury. It was created on the basis of assets of Polska Poczta, Telegraf i Telefon – State operator of all telecommunication services before systemic transformation in 1989. TP S.A. never had legal monopoly, but its *de facto* monopolist status was therefore inherited.

[307] M. Szydło, *Umowy w sprawach dostępu do sieci telekomunikacyjnych*, Rejent (10)2006; S. Piątek, *Rozporządzenie UE Nr 2015/2120 w zakresie dostępu do otwartego internetu. Komentarz*, C.H. Beck 2017, p. 29.

[308] J. Kowalski, *Zasada neutralności sieci a relacje pomiędzy dostawcami kontentu i usług internetowych (ISP*, Czas Informacji (2)2010, p. 17; M. Danek, *European Commission's decision in Telekomunikacja Polska as an example of application of the Guidance on exclusionary abuses of dominant position*, Zeszyty Naukowe Uniwersytetu Jagiellońskiego (3)2013, pp.139-146.

This regulatory challenge was largely rendered irrelevant with the abolition of *de facto* network monopoly[309].

As of zero-rating [translated in the Polish version of the BEREC Guidelines as *stawka zerowa*] in Poland, there are no dedicated regulations[310]. However late 2015 the Office of Electronic Communications expressed the view that zero-rating could affect customers' freedom of choice and thus should be closely monitored[311]. Under existing rules mentioned office is tasked to safeguard net neutrality and can impose fine on the infringing operator[312]. Additionally, like all trade practices charging zero-rating can be controlled by the competition authority. Under certain circumstances, it could be considered an abuse of dominant position[313]. Additionally zero-rating may constitute an act of unfair competition aimed at squeezing competition out from the market[314]. These interpretations are valid from a legal standpoint but so far remain purely theoretical. Nevertheless, existing regulatory framework seems to be sufficient when it comes to combating possible adverse effects of zero-ratings.

Question 3.2.

Development of digital infrastructure in Poland is primarily done under Operational Program "Digital Poland 2014-2020" [pol. *Program Operacyjny Polska Cyfrowa 2014-2020*] which falls under EU Regulation 1303/2010. The program co-financed by the European Regional Development Fund consists of four parallel priority axis: universal access to the fast internet; e-administration and open government; digital competences of the society; technical assistance[315]. In 2014

[309] In 2007 TP S.A. subjected to unbundling where its upstream and downstream activities were functionally separated. R. Śliwa, *Separacja operatora telekomunikacyjnego – narzędzie regulacyjne: przypadek sektora telekomunikacyjnego w Polsce*, Ekonomia i Prawo (8)2012, pp. 211-225.

[310] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, 30.08.2016, BoR (16) 127, para 40.

[311] Stanowisko Prezesa UKE w sprawie środków dotyczących dostępu do otwartego internetu, ustanowionych w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r.

[312] Article 209(29a) of the Telecommunication Law. M. Czyżak, *Kara pieniężna jako instrument regulacji rynku telekomunikacyjnego*, internetowy Kwartalnik Antymonopolowy i Rregulacyjny (6)2012, pp. 20-30

[313] Rules preventing abuses of dominant position encapsulated in Article 9 of the Polish Act on Competition and Consumer Protection are fashioned after Article 102 TFEU and analogous rules of interpretation applies. See inter alia C. Banasiński, E. Piontek (eds.), *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, LexisNexis 2009.

[314] Article 3(1) of the Act on Combating Unfair Competition defines act of unfair competition as any behaviour that threatens or infringes interest of another trader. See on interpretation of this notion M. Sieradzka, M. Zdyb (eds.), *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz, wyd. II*, Wolters Kluwer 2016.

[315] Official document *Szczegółowy opis osi priorytetowych Programu Operacyjnego Polska Cyfrowa na lata 2014-2020* prepared by the Ministry of Development is available at: https://www.polskacyfrowa.gov.pl/media/31464/POPC_SZOOP_30122016.pdf (11.05.2017).

Council of Ministers adopted a policy document entitled Poland's National Broadband Plan [pol. *Narodowy Plan Szerokopasmowy*] which set a goal that 100% of households and companies should have access to internet connectivity of which at least 30 Mbps until 2020 and 50% of households and businesses have access to internet connectivity of 100 Mbps until 2020[316]. Additionally generic Construction Law requires every zoning plan to include access points for broadband internet[317]. Furthermore mentioned Act contains the delegation of authority to a relevant minister to set technical requirements for newly constructed building and other objects[318]. In 2010 legislator went further and through an amendment to Construction Law currently, all residential, as well as public buildings are *ex-lege* required to have installations enabling hooking up broadband internet[319]. Of other notable initiatives, program „Nationwide Education Network [pol. *Ogólnopolska Sieć Edukacyjna* – OSE] requires mentioning. Launched in December 2015 the program set a goal to provide broadband access to every school in the country by the end of 2018[320].

Finally, It is hard to answer the question whether EU should go further in creating a single digital market if there are no specific legislative proposals put forward. Looking at it from the standpoint of infrastructure construction and operation, the author sees no obvious *ratio legis* nor necessity for any particular regulation. It is also worth noting that there is already quite a significant *acquis* in competition law dedicated to principles of equal and non-discriminatory access to various infrastructures (including telecommunications) which, to a large extent, are relevant here.

Question 3.3.

In Poland Article 26(6) of the Broadcasting Act contains a provision establishing President of the Office of Electronic Communications competence to reserve

[316] Policy document National Broadband Plan [pol. *Narodowy Plan szerokopasmowy*] prepared by the Ministry of Administration and Digitalisation is available at: https://mac.gov.pl/files/narodowy_plan_szerokopasmowy_-_08.01.2014_przyjety_przez_rm.pdf (11.05.2017)/

[317] Construction Law [*Ustawa z dnia 7 lipca 1994 r. – Prawo budowlane*], Dz.U. 1994 nr 89 poz. 414, Consolidated Version Dz. U. z 2016 r. poz. 290, 961, 1165, 1250, 2255.

[318] A. Gliniecki (ed.), *Prawo budowlane. Komentarz, wyd. II*, Wolters Kluwer 2014, pp. 112-113; A. Plucińska-Filipowicz, M. Wierzbowski (eds.), *Prawo budowlane. Komentarz, wyd. II* Wolters Kluwer 2015, pp. 16-17 and 182-185; Ł. Strzępek, *Kilka uwag na temat szczególnych zasad lokalizowania inwestycji telekomunikacyjnych w miejscowym planie zagospodarowania przestrzennego*, Przegląd Prawa Publicznego (5)2013, pp. 41-51.

[319] Amendment introduced Article 5(2a) to the Construction Law. It was done by Article 65(2) of the Act on May 7th 2010 on Supporting Development of telecommunication Networks [*ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych*] Dz.U z 2010 nr.106 poz. 675.

[320] Outline of the draft proposal is published by the Ministry of Education [pol. *Ministerstwo Edukacji*]. Documents are available at: https://men.gov.pl/ministerstwo/informacje/ogolnopolska-siec-edukacyjna-zalozenia-do-projektu-ustawy.html (11.05.2017)

certain frequencies for public broadcasters – namely TVP 1, TVP 2, and regional channels[321]. Article 26(7) extends frequency reservation requirement to TVP Polonia (targeted at Polish-speaking audiences outside Poland) which is broadcasted chiefly via satellite[322].

Spectrum management in regards to other channels – both satellite and terrestrial – is regulated by the Article 115(3) of the Telecommunication Law. Reservation of spectrum requires requesting operators to submit list of programmes on a given multiplex; description of proportion between various programmes in one multiplex; delimitation of broadcasting's territorial scope; information on bandwidth usage[323]. President of the Office of Electronic Communications is responsible for issuing changing and withdrawing of reservation decisions[324].

It is not entirely clear whether above rules apply only to public broadcasters specified in Articles 26(6), and 26(7) of the Broadcasting Act or do these also cover so-called "specialised programmes" [pol. *programy wyspecjalizowane*][325]. This category of content defined in Article 4(13) of mentioned act as a programme in which no less than 70% of the monthly content transmitted between 6AM-11PM is specialization-related[326]. It is not always the case, but these programmes often fall under public service mission[327]. If one would assume that mentioned Article 115(3) of the Telecommunication Law applies that every programme in public broadcaster's telecast, it would be entirely exempted from licensing requirements [pol. *koncesja*][328]. This distinction between policy-oriented and supply-oriented paradigms of spectrum management is often blurred in practice, but former approach is perilous as bearing a resemblance to preventive censorship[329]. The

[321] K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, LEX Wolters Kluwer business 2015, p.149-151.

[322] K. Chałubińska-Jentkiewicz, *Audiowizualne usługi medialne...*, p. 279.

[323] J.A. Krasucki, *Prawo telekomunikacyjne. Komentarz, wyd. IV*, Wolters Kluwer 2015, p. 976-981.

[324] A. Krasucki, *Postępowanie w sprawie zmiany rezerwacji częstotliwości*, Przegląd Ustawodawstwa Gospodarczego (6)2016, pp. 17-29.

[325] E. Czarny-Drożdzejko, *Ustawa o radiofonii i ...*, p. 310-314/

[326] M. Rogalski (ed.), *Prawo telekomunikacyjne*, LEX Wolters Kluwer business 2011, pp.

[327] This is implicitly recognized by the National Broadcasting Council in Regulation of May 18th 2016, on the lower ratio of Polish language auditions, and European auditions in TV and Radio programmes in Polish [*w sprawie niższego udziału w programie telewizyjnym audycji wytworzonych pierwotnie w języku polskim i audycji europejskich oraz w programie radiowym utworów słowno-muzycznych wykonywanych w języku polskim*], Dz.U. z 2016 nr 779.

[328] Article 115(3) of the Telecommunication Law stipulated that „reservation" of frequency is done through the decision of President of the Office of Electronic Communications.

[329] In Poland any form of preventive censorship in media is explicitly prohibited by the Article 54 of the Constitution. See *inter alia* E. Czarny-Drożdżejko, *Zakaz publikacji jako zabezpieczenie powództwa w sprawach cywilnych skierowanych przeciwko prasie*, Przegląd Sądowy (1)2014, pp. 37-57; W. Sokolewicz, *Prasa i Konstytucja*, Wolters Kluwer Polska 2011.

regulatory framework is therefore not coherent. Because public service obligation ("public mission" in literal translation of Polish notion *misja publiczna*) is discharged *inter alia* through "specialised programmes". So the system is redundant as license procedure, primarily aimed at achieving public interest goals, is required for these programmes[330]. At the same time, it was mentioned, undertakings with the status of public broadcasters are exempted from separate licensing requirements, and have a privileged allotment of spectrum solely of the basis of being entrusted with public service obligation[331].

Question 3.4.

Arguably the most contentious issue relating to regulator's impartiality is caused by the blurred division of competencies of National Broadcasting Council [pol. *Krajowa Rada Radiofonii i Telewizji*] and Office of Electronic Communications [pol. *Urząd Komunikacji Elektronicznej – UKE*]. The former institution's competencies and composition were analysed in question 2.4.

As of latter body, the Office enjoys the status of central government[332]. The Office's President is appointed for the five-year term by the Sejm of the Republic of Poland, with the consent of the Senate[333]. The President cannot be dismissed by the appointing bodies and can only be removed from office in case of manifest infringement of law; conviction for a deliberately committed offence or fiscal offence; illness; voluntary resignation[334]. The Office's President does not resign when appointing government resigns[335]. The activities of the President of UKE are currently supervised by the Minister of Digital Affairs and in the area of postal services by the Minister of Infrastructure and Construction[336].

To sum up, legal safeguards of Polish national regulatory authority – Office of Electronic Communications, are not in question. There are also no major controversies on how the Office is performing its tasks.

330 K. Chałubińska-Jentkiewicz, *Audiowizualne usługi medialne...*, pp. 280-281.

331 Ibidem.

332 Article 3 of the Act of December 29th, 2005 on transformations and changes in the division of tasks and competences of state bodies competent in matters of communications, radio and television [*Ustawa z dnia 29 grudnia 2005 r. o przekształceniach i zmianach w podziale zadań i kompetencji organów państwowych właściwych w sprawach łączności, radiofonii i telewizji*], Dz.U. 2005 nr 267 ze zm.

333 Article 190(4) of the Telecommunication Law.

334 J.A. Krasucki, *Prawo telekomunikacyjne....*, p. 1469-1477; M. Rogalski, *Zmiany w prawie telekomunikacyjnym. Komentarz*, Wolters Kluwer Polska 2006, pp. 220-228.

335 S. Piątek, *Prawo telekomunikacyjne...*, p. 1042

336 Article 189(1) of the Telecommunication Law.

4. Data in the digital economy

Question 4.1.

The principal preparatory activity for the upcoming GDPR comprises of a comprehensive revision of existing data protection regulations. Although in EU law Regulations are directly applicable the GDPR contain numerous referrals to national legislations as well as various exemptions requiring recourse to domestic rules hence a certain legislative adaptation is required[337]. There was a debate whether current Personal Data Protection Act should be amended or shall more comprehensive approach be taken, and the act replaced altogether. Finally, legislator chooses the latter option and currently draft version, prepared by the Ministry of Digitalisation is undergoing consultation[338].

Additionally, it is estimated approximately 600 acts currently in force requires reviewing whether they are GDPR-compatible[339]. This part could prove to be problematic. The Ministry of Digitalisation which is tasked to prepare the reform of generic data protection rules have neither competencies nor resources to conduct a review of all sector-specific regulations, so these efforts lack any centralised guidance[340]. It is, therefore, hard to predict how each department would approach this issue and what legislative proposals would be put forward. The quality and overall cohesion of these scattered sector-specific future initiatives are unknown. Yet the perspective is not especially optimistic as Polish lawmakers often failed to ensure GDPR compatibility for acts enacted during Regulation's *vacatio legis*[341].

[337] On the regulatory model see W. Wiewiórowski, *Nowe ramy ochrony danych osobowych w Unii Europejskiej*, in: G. Sibiga (ed.), *Aktualne problemy ochrony danych osobowych 2012*, dodatek do Monitora Prawniczego (7)2012, pp. 3 et seq.

[338] Draft version is available at the Ministry's website at: https://mc.gov.pl/files/projekt_ustawy_o_ochronie_danych_osobowych_28.03.2017.pdf (14.05.2017).

[339] This figure was provided initially provided in 2015 by the acting Inspector General for Personal Data Protection Andrzej Lewiński, later it has been repeated in official policy documents published at the Inspector's website.

[340] In reply to parliamentary interpellation no. 4764 of 17.08.2016 [*Odpowiedź na interpelację nr 4764 w sprawie implementacji do polskiego systemu prawa przepisów rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* BMP-0713-l-92/2016/PS] the Minister of Digitalisation Anna Streżyńska expressed opinion that the ministry see no reason to appoint a specific working group to coordinate implementation efforts, although *ad hoc* consultations will be held should the need arises.

[341] Two examples are especially glaring requiring mentioning: First Act of February 11th on the State assistance for bringing up children [*Ustawa z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci*, Dz.U. 2016 poz. 195, Consolidated version Dz. U. z 2016 r. poz. 195, 1579. colloquially called 500+ due to the amount of allowance for each child] introduces completely new concept of collective data administrator and excludes requirement for specific agreement for transfer of personal data

Additionally the Inspector General for Personal Data Protection is organising information campaign aimed at raising awareness of upcoming changes. These include among other things conferences, workshops, training sessions[342]. The Inspector also organised an experts' committee tasked with providing analytical assistance to planned legislative initiatives[343].

Question 4.2.
It is impossible to answer this question due to insufficient data aggregation. No official statistics is showing the level of preparedness for the new GDPR, although there is highly doubtful whether such comprehensive report could be compiled due to methodological obstacles. There are however numerous of commercial reports painting a bleak picture[344]. These documents show a widespread lack of awareness of the nature of new rules especially regarding reporting of data security breach. Notwithstanding these non-official reports are authored by the companies providing data security solutions, therefore, their accuracy, methodology and overall analytical value are questionable at best. It is conjecture but judging from the number of training commercially offered by various companies which indicated an existence of a quite brisk market of GDPR-preparedness solutions, a significant demand among undertaking can be assumed. In turn, this could be perceived as a proof (or at least indication) of awareness among business persons to the GDPR requirements. As mentioned before, these observations are not based on any official statistics (which are non-existent) and thus should be treated warily.

Question 4.3.
In Poland, there is quite an extensive debate on the Internet of Things [pol. *Internet rzeczy*] although the majority of public attention is focused on technical rather than legal challenges of this phenomenon. It does not mean that there is no legal debate, but it is more fragmented as selected, specific issues are often analysed without labelling them as part of the wider concept of Internet of things.

provided transfer is done between public bodies. Second act of September 25th 2015 o amendment of the Freedom of Economic Activity Act and other acts [*Ustawa z dnia 25 września 2015 r. zmianie ustawy o swobodzie działalności gospodarczej oraz niektórych innych ustaw*, Dz.U. 2015 poz. 1893] which partially excluded application of Personal Data Protection Act to registries of business activity [pol. *ewidencja dzialalnosci gospodarczej*].

342 Information about Inspector's activities on this field are published in its official website at: http://www.giodo.gov.pl/1520278/j/pl/ (12.05.2017).

343 The Inspector General for Personal Data Protection do not have right of legislative initiative in itself but is participating in law making in advisory capacity.

344 These will not be quoted to avoid advertising.

If one would look at the areas that fall under the umbrella category of Internet of Things there are following the topic of the policy debate that raises legal issues:

Data protection in telecommunication services: In principle Article 159(1) of the Telecommunication Law guarantees the confidentiality of information regarding individual's transmission data, localisation, sent information, connections attempts between various terminals[345]. These apply to both natural persons and institutional users[346]. The confidentiality requirement bounds service providers and legal obligation are created during entering into a contract with a given end-user[347]. This regime seems to be too inflexible if it comes to data collected by various devices not for the explicit purpose of gathering, but through their normal operations[348]. Individuals operating these devices do not have the status of telecommunication undertakings and thus are outside mentioned data protection regime. In this case, generic data protection rules should be applied[349].

Data anonymisation in smart cities: It stands to reason that efficient collection and processing of information can significantly enhance quality, performance and interactivity of municipal services allowing for real-time responses, managing urban flows and so forth[350]. The primary problem arising with smart cities in relation to use of data to enhance the functioning of various urban systems stems from the legal status of the data in itself[351]. Existing regulations are seriously

[345] A. Krasucki, *Prawo telekomunikacyjne...*, pp. 1296-1305; A. Krasuski, *Podstawy prawne przetwarzania danych objętych tajemnicą telekomunikacyjną*, Przegląd Ustawodawstwa Gospodarczego (8)2016, pp. 2-12; M. Siwicki, *Ochrona praw autorskich, bezpieczeństwa systemów informatycznych, danych osobowych i tajemnicy telekomunikacyjnej w chmurach obliczeniowych*, Prokuratura i Prawo (5)2015, p. 110.

[346] The wide subjective scope of this right stems from the fact that provision in question directly reflects the principle of "freedom and confidentiality of communication" [pol. *wolność i ochronę tajemnicy komunikowania się*] enshrined in Article 49 of the Constitution. See W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Wydanie VII*, LEX Wolters Kluwer business 2013, p. 59 et seq.

[347] There is no need for explicit individual's consent for processing of transmission data. There is a legal presupposition that such consent exists provided individual was fully aware of processing in question and do not specifically disagreed to it. See A. Krasuski, D. Skolimowska, *Dane osobowe w przedsiębiorstwie*, LexisNexis 2007, p. 59.

[348] A. Adamski, *Retencja danych o ruchu telekomunikacyjnym – polskie rozwiązania i europejskie dylematy*, Przegląd Prawa i Administracji (LII)2005, pp. 173-188.

[349] S. Piątek, *Telekomunikacja a Internet rzeczy* in: G. Szpor (ed.), *Internet rzeczy. Bezpieczeństwo w Smart city*, C.H. Beck 2015, pp. 25 et seq.

[350] It goes without saying that there is no legal definition of „Smart Cities", as the concept functions in numerous field of science – IT, social sciences, law, to name just a few. For the purpose of this analysis the notion will be used in the meaning of definition provided by Wikipedia according to which it is "(...) urban development vision to integrate information and communication technology (ICT) and Internet of things (IoT) technology in a secure fashion to manage a city's assets" (https://en.wikipedia.org/wiki/Smart_city 05.05.2017).

[351] S. Piątek, *Telekomunikacja a Internet...*, p. 26; P. Piątek, S. Piątek, *Anonimizacja danych objętych tajemnicą telekomunikacyjną*, internetowy Kwartalink Antymonopolowy i Regulacyjny (3)2014, pp. 47-61.

lacking if it comes to anonymisation of data because only localisation data can be anonymised and thus later processed without specific and explicit consent[352]. It has to be noted that Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector is equating anonymisation of data with its removal[353]. Similar regulation is missing in Polish legal order. Instead, domestic regulations in Telecommunication Law had generally introduced more stringent regime for data protection in telecommunication services especially provision which held that data collected in the process of providing communication services could be only used for the operation of these particular services[354]. It is therefore not possible to export anonymised data to feed some urban systems thereby improving their data aggregation. At the same time, at least in principle, under generic data protection regime anonymised information is not regarded as "personal data" [pol. *dane osobowe*] anymore[355]. The very operation of anonymisation is also not qualified as "processing" [pol. *przetwarzanie*] in the meaning of Personal Data Protection Act[356]. So the administrator is free to anonymise personal data and transfer this non-personal data to any entity at its discretion. In this context, the problem with telecommunications lies somewhat paradoxical in the Personal Data Protection Act. The act contains general clause according to which generic data protection rules are inapplicable if sectoral regime provides "more extensive" [pol. *dalej idące*] guarantees[357]. The issue remains controversial as the meaning of "more extensive" is debatable in itself, especially one could convincingly argue that "differently" is not synony-

[352] Article 166(1) of the Telecommunication Law; A. Krasucki, *Prawo telekomunikacyjne*..., pp. 1327-1328; P. Koralewski, *Usługi oparte na przetwarzaniu danych geograficznych*, internetowy Kwartalink Antymonopolowy i Regulacyjny (6)2012, pp. 58-73.

[353] Article 6 of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

[354] S. Piątek, *Telekomunikacja a Internet*..., p. 26.

[355] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, LEX Wolters Kluwer business 2015, p. 263; P. Barta, J. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, C.H. Beck 2016, pp. 56-60.

[356] This was initially stated by the Court of Appeal in Gorzów, 22.03.2012, II SA/Go 48/12. Later this line of reasoning has been picked up and applied in numerous cases *inter alia* by the Voivodship Administrative Court in Warsaw, 03.11.2015, II Sa/Wa 723/15.

[357] Article 5 of the Data Protection Act. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych*..., pp. 298-299. Application of this provision requires case-to-case analysis. There is quite extensive case-law of Polish courts on this matter. Following rulings are especially instructive (although list is by no means exhaustive): Judgment of Supreme Administrative Court in Warsaw, 19.05.2010, I OSK 1029/10; 30.07.2009, I OSK 1115/08; 26.01.2009, I OSK 174/08. See further A. Kisielewicz, *Ochrona danych osobowych w praktyce orzeczniczej Naczelnego Sądu Administracyjnego*, Glosa (2)2001, pp. 32 et seq.

mous with "more comprehensive", and broadly speaking "better"[358]. It is exactly the case here, and additionally, there is no clear-cut reason why data subjected to prior anonymization collected through the provision of telecommunication services should not be used for other purposes[359].

Liability for autonomous/semi-autonomous systems: Although in Poland there is no specific legal liability regime for autonomous or semi-autonomous systems (aerial, terrestrial, marine) generic rules encapsulated in the Civil Code [pol. *Kodeks Cywilny*] are applicable. The first issue that comes up in this context is the level of real autonomy of a given device. According to general civil law-based principle, liability can occur only if there is a "causal connection" between certain behaviour and harm[360]. It is glaringly obvious that such link is non-existent (or at least not obvious) if the machine can act independently[361]. However, the problems do not end here as the devices' activity could as well be fed corrupted information affecting its decision algorithms, or sensors could be faulty or damaged, or finally, some third party could have taken control of a device[362]. Introducing rules for liability on risk basis [pol. *odpowiedzialność na zasadzie ryzyka*] brings more practical value but it leaves no room for exoneration if damage/harm had been done due to circumstances outside person's control (i.e. non-detectable faults in equipment)[363]. It however only applies to individually owned devices. If autonomous systems belong to an undertaking, liability regime for so-called "motion of an undertaking" [pol. *ruch przedsiębiorstwa*] encapsulated by the Article of 435 of the Civil Code could be applicable[364]. The provision exempted entrepreneur's liability for activities of its assets only in case of *vis maior* and

[358] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, p. 300.

[359] S. Piątek, *Telekomunikacja a Internet...*, p. 26.

[360] K. Osajda (ed.), *Kodeks cywilny. Komentarz. Tom II. Zobowiązania (art. 353-921[16] KC*, C.H. Beck 2013, pp. 790-791. It is emphasized in the doctrine that liability can be assumed for "own act" [pol. *czyn własny*] of an individual. However definition of individual "act" [pol. *czyn*] could be controversial in some cases: W. Czachórski, *System prawa cywilnego, tom III, cz. 1*, INP PAN, Ossolineum 1976, p. 528; A. Olejniczak (ed.), *System Prawa Prywatnego. Tom 6, Prawo zobowiązań – część ogólna*, C.H. Beck 2014, pp. 385 et seq.

[361] It is worth to mention that Article 431 of the Civil Code introduces specific liability regime for damages caused by individual's animals, which in practice could be non-controllable or at least difficult to control. The provision obviously cannot be applied to UAVs, but this model of liability could provide a useful template for future legislative initiatives.

[362] There is considerable body of research work outlining technical possibility of either taking control over UAV or feeding it with corrupted data to disrupt operation. See *inter alia* A.J. Kerns, D.P. Shepard, J.A. Bhatti, T.E. Humphreys, *Unmanned Aircraft Capture and Control Via GPS Spoofing*, Journal of Field Robotics, Special Issue: Special Issue on Low Altitude Flight of UAVs 31(4)2014, pp. 617-636 K. Wesson, T.E. Humphreys, *Hacking Drones*, Scientific American (309)2013, pp. 54-59.

[363] It can be argued that if technical fault was detectable (with due diligence) then the operator could be held liable for the lack of proper maintenance.

[364] K. Osajda (ed.), *Kodeks cywilny...*, pp. 586-594.

due to full involvement of the third party[365]. Additionally, it can be argued that owners of autonomous devices (word "operator" seems to be ill-fitting is system is indeed autonomous) could be held liable though regime designed for "dangerous products" [pol. *Produkt niebezpieczny*][366]. To reiterate, existing regulations do provide general rules for legal liability but are lacking clarity when it comes exoneration and transferring liability[367].

Question 4.4.

Polish Constitution contains a general principle of personal data protection[368]. The general rule is fleshed out in Personal Data Protection Act which contain a provision under which an individual can request removal collected personal data provided these are "incomplete, outdated, inaccurate, collected in violation of law, unnecessary for the purpose which they were collected"[369]. Current regulations (as of 21.04.2017) do not allow removing data that are factually correct and legally collected (either by individual's consent or *ex lege*)[370]. Which conjures up the question of whether situation similar to *Costeja* case date could fall within the remit of "outdated" criterion. It is doubtful given that information in question are not incorrect, and reflect factual circumstances at the time of data collection, so these are not subject to expiry[371]. Otherwise virtually all historical – not current – information could be delisted under this criterion. In the same

[365] To successfully exonerate liability it must be proven that given activity that had led to damage is fully attributable to a third party. See Judgment of Supreme Court, 08.11.1988, II CR 315/88, OSP 1990, z. 4, poz. 217; 06.07.1973, II CR 156/73, OSP 1974, z. 5, poz. 95. See also J. Jastrzębski, *Interferencje adekwatnej przyczynowości oraz winy przy odpowiedzialności za szkodę majątkową*, Przegląd Sądowy (7-8)2004, pp. 26-29.

[366] Article 449[1](3) of the Civil Code. C. Żuławska, *Ewolucja odpowiedzialności za jakość świadczenia*, in: E. Łętowska (ed.), *Tendencje rozwoju prawa cywilnego*, Ossolineum 1983, p. 240

[367] Drones are exempted from general aircraft insurance requirements although there is specific liability insurance requirements for drones of MTOW (maximum take-off weight) 5 – 20kgs.

[368] Article 51 of the Constitution. M. Haczkowska (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, LexisNexis 2014, pp. 81-82; W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Wydanie VII*, LEX Wolters Kluwer business 2013, pp. 60-61.

[369] Article 35(1) of the Personal Data Protection Act.

[370] W. Dubis, M. Daćków, *Prawo do bycia zapomnianym w internecie – za życia i po śmierci?*, in: D. Karkut, J. Mazurkiewicz, J. Gołaczyński, J. Turłukowski (eds.), *Non omnis moriar: osobiste i majątkowe aspekty prawne śmierci człowieka: zagadnienia wybrane*, WUWr 2015, pp. 177-178. It can be argued that mentioned provision contain a right to update personal data so according to this line of reasoning outdated information should be altered accordingly. This interpretation is tenuous at best. See J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz, wydanie VI*, LEX Wolters Kluwer business 2015, p. 540.

[371] See K. Święcka, *Kryterium prawdziwości wypowiedzi a ochrona dóbr*, Ruch Prawniczy, Ekonomiczny i Socjologiczny 73(4)2011, pp. 53-69.

vein anti-defamation [pol. *zniesławienie*], and personal rights protection [*ochrona dóbr osobistych*] rules contained in Civil Code are equally inapplicable[372].

There've been no legislative initiatives in Poland as a direct result of *Costeja* case, but it is said then in similar cases an individual could anchor his/her claim directly on Articles 7 and 8 of the Charter of Fundamental Rights[373]. It is also argued that fundamental law-based concerns should trump economic interest of data administrator. However, since there are no comparable cases in national courts – when Charter was directly invoked as a sole basis for the claim – it is hard to judge as to how the balance between these contradicting goals will be struck, especially in light of *Węgrzynowski and Smolczewski v. Poland* ECHR ruling which essentially contain interpretation opposite to *Costeja* CJEU's case[374].

[372] Polish law do not differentiate between libel and slander. Websites such as forums or newspaper's websites are not considered to be a Collections of Personal Data [pol. *zbiór danych osobowych*] as per Article 7(1) of the Personal Data Protection, and thus information stored on these media cannot be removed as per Article 35(1) of the Personal Data Protection Act, but instead it is necessary to invoke civil-law-based rules of personal rights protection encapsulated in Article 23 of the Civil Code. See M. Ilnicki, *Prawo do bycia zapomnianym w kontekście „poszniesławiającej" informacji w sieci Internet, cz. 1*, Palestra (1-2)2014, pp. 132-13; M. Ilnicki, *Prawo do bycia zapomnianym w kontekście „poszniesławiającej" informacji w sieci Internet, cz. 2*, Palestra (5-6)2014, pp. 99-107.

[373] W. Dubis, M. Daćków, *Prawo do bycia...*, p. 180; M. Krzysztofek, *„Prawo do bycia zapomnianym" i inne aspekty prywatności w epoce Internetu w prawie UE*, Europejski Przegląd Sądowy (8)2012, pp. 29-34.

[374] Case *Węgrzynowski and Smolczewski v. Poland*, Application no. 33846/07

PORTUGAL

Manuel Lopes Rocha
Gonçalo Machado Borges
Magda Cocco

1. Internal Market and electronic commerce : Internet and e-commerce
1.1. Electronic Commerce, liability of Internet intermediaries

Question 1.1.1.
The Portuguese legislator transposed the E-Commerce Directive by means of Decree-Law 7/2004, of 7 January (the "E-Commerce and Data Protection Act"). In what concerns the liability of intermediary service providers, and notwithstanding the fact that Decree-Law 7/2004 has been subjected to two amendments, in 2009 and 2012, respectively, the wording of the relevant legal provisions remains the same as it did back in 2004.

During this period, some difficulties in interpreting the law have indeed been noticed, as is expected when it comes to a decade-old act that governs an ever-changing digital world.

That being said, and in what specifically concerns the definition of 'intermediary service providers', for instance, (which, one should note, is absent from the E-Commerce Directive) Portuguese courts have not strayed away from what is laid down on Article 4 of Decree-Law 7/2004 – "*'Intermediary service providers' are those that provide technical services enabling the access, provision and use of information or of online services that are independent from the very own content creation or the establishment of the services they make possible*".

As a result, the scope of 'intermediary service providers' in Portugal is quite consensual (as the Portuguese legislator put forward a definition of 'intermediary service providers', something that did not figure in the E-Commerce Directive)

although, at the same time, it is also quite broad – ISPs, web hosts, sharing websites, and others, are all taken as being 'intermediary service providers', as was envisaged by the E-Commerce Directive. Crucially, however, there is also some leeway to argue that, under Decree-Law 7/2004, social network websites, for instance, or *peer-to-peer* trackers (e.g. BitTorrent trackers, that assist in the communication between different users using the BitTorrent protocol) also act in the market vested with that quality.

It would therefore seem that the difficulties that arise out of Decree-Law 7/2004, and that involve the concept of intermediary service providers, are not intrinsically related to 'definitions' but are 'material' concerns instead. The crux of the matter is therefore what is or is not expected from intermediary service providers, as well as to who are, exactly, these intermediary service providers, bearing in mind the definition set out in Decree-Law 7/2004.

In saying this, we refer, of course, to the liability exemption provisions found in Article 13, 14 and 15 and to the correlated absence of a general monitoring obligation by intermediary service providers as laid down in Article 12 of Decree-law 7/2004, all derived from Article 12, 13, 14 and 15 of the E-Commerce Directive, respectively.

Whereas the E-Commerce Directive provided for the non-existence of a 'general obligation to monitor' in respect of providers qualifying as 'mere conduit', 'cache' and 'hosting', the Portuguese legislator instead prescribed a general exemption for all those who qualify as 'intermediary service providers', as per the definition above.

The broadness of the definition of 'intermediary service providers', as laid down on Article 4 of Decree-Law 7/2004, theoretically means that, under Portuguese law, it is possible for providers, that would otherwise not fall under the scope of Article 12, 13 and 14 ('mere conduit', 'cache' and 'hosting', respectively) of the E-Commerce Directive, to nevertheless be exempted from a duty to monitor under Portuguese law, thus making any case for their possible liability more difficult to argue (as no monitoring obligation is borne by them).

This is particularly troublesome when we bear in mind the fact that, in Portugal, as previously mentioned, one of the criteria used for establishing whether an entity is as an intermediary service provider involves an assessment of whether those technical services that are being provisioned are "*independent from the very own content creation or the establishment of services they make possible*".

In extremis, a disproportionately great number of crucial 'technical services' rendered online may be "*independent from the very own content creation*". An automated, or quasi-automated, online repository of hyperlinks and/or .torrent files, all of them uploaded by site users, could nonetheless be 'independent' from content creation or from the establishment of the services they allow for (e.g. the

download of unlawful content), and would therefore not be the subject of a general monitoring obligation.

Likewise, e-commerce hubs, social-networks, and other platforms that do play an active role over content by optimising the presentation of said content and even by imposing formal requirements over them, would also be exempted of such duty due to the fact that, ultimately, whatever role they play over that content does not preclude the fact that they are indeed "*independent from [...] content creation or the establishment of the services they make possible*".

This wording (and reading) of Portuguese law, that goes beyond what is prescribed in the E-Commerce Directive, is, naturally, troublesome, especially so in light of L'Oréal v eBay, C-324/09 (see below), as the CJEU found eBay, an online marketplace, not to be an 'intermediary service provider' because it did not take a neutral position between the customer-seller (in the sense it helps the seller promote its products and even imposes restrictions on their presentation). By placing the yardstick on a service's 'independence' from the *creation* of the end content and/or services, the provisions found on Decree-Law 7/2004, in what concerns intermediary service providers' liability may be found as being in opposition to the outcome of L'Oréal v eBay.

Question 1.1.2.

Our understanding is that, in L'Oréal v eBay, the CJEU has put forward a reasonable test for liability and has helped clarify the exact extent of the 'Hosting' defence – something of particular importance for Portugal in light of the aforementioned troublesome wording of the provisions that transpose the E-Commerce Directive.

More importantly, the CJEU's test for liability in L'Oréal v eBay has made it clear that the cornerstone of the Hosting defence is based on whether the provider has taken a neutral position between the background relationship (e.g., *in casu*, the costumer-seller relationship).

We understand that this reading of the Hosting defence may also inform all available defences under the E-Commerce Directive as well as, obviously, under all national acts that transpose said Directive.

In other words, notwithstanding the individual conditions laid down under each one of the liability exemptions found in Article 12 et seq. of the E-Commerce Directive, the underlining rationale is that, for the intermediary service provider to be exempted of liability, it shall act neutrally regarding the data provided and processed by its recipients. Therefore, as the CJEU recapped, where a service provider *"instead of confining itself to providing that service neutrally by a merely technical and automatic processing of the data provided by its customers, plays an active role of such a kind as to give it knowledge of, or control over those data*", namely by *"optimising*

the presentation of the offers for sale in question or promoting those offers", said service provider cannot be considered but a non-neutral provider, and therefore general rules on its liability shall apply.

Our take on this matter is that this line of reasoning may also be applicable to the two other defences under the E-Commerce Directive – the 'mere conduit' and 'cache' defences – insofar one properly adapts this rationale.

In other words, it is very well possible for a 'mere conduit' not to act neutrally regarding eventual unlawful acts by its consumers (only has to think of the growing number of VPN service providers that spoof consumer IPs and specifically cater to those who wish not to get caught downloading illegal content, going as far as providing complex payment mechanisms that 'whitewash' payments for using those services) and the same goes for certain caching services.

It is true that the E-Commerce Directive did bear in mind these circumstances to some extent, but in doing so emphasis was placed on 'deliberate collaboration' with service recipients in order to undertake illegal acts (see Recital 44 of the E-Commerce Directive). L'Oréal v eBay, however, seems to point out that 'malicious neglect' also will not be covered by any of the three liability exemptions found in the E-Commerce Directive. If you run a service, as an intermediary, in which you allow for, and foster (even if only indirectly) illegal acts to be undertaken by its recipients, your liability will not be exempted *per se* and it shall be assessed in light of general liability rules, regardless of whether you did have direct interference in the end contents and/or services or not.

We see this nuanced reading of the E-Commerce Directive as being paramount as an update effort under the auspices of Digital Single Market reform. We also understand that reducing the number of 'liability shields' available for intermediary service providers makes sense in light of today's concerns and the growing infiltration of the online world in everyday life. In fact, it might even help for more timely solutions regarding breaches of law without resorting to more draconian measures of control and web surveillance (as intermediary service providers will feel hard-pressed into acting quickly and responsibly upon gaining knowledge of an illegal situation).

Finally, we cannot help but refer to João Fachana's reading of how the E-Commerce Directive liability exemption regime was based in three, now arguably outdated, distinct pillars: (i) that it was unfeasible for intermediary service providers to effectively advance control over the contents uploaded and transmitter through their services; (ii) the typical neutrality of ISP's with respect to third-party contents; (iii) that an overactive liability regime could hinder internet access, propagation and, in our understanding, also e-commerce/cross-border commerce.[1]

[1] "ISP Secondary Liability – A Portuguese Perspective on Omissions as the Basis for Secondary Liability", João Fachana in Secondary Liability of Internet Service Providers, Springer, 1st ed. 2017

Indeed, it does seem that many of these pillars have been shattered or are, at the very least, trembling.

Mass data filtering technology has matured immensely during the past decade, and ISPs have abandoned their typical neutral stance towards third-party contents (one only needs to consider the net neutrality debate), and, of course, even more strikingly, the internet is pretty much everywhere these days – to the point that e-commerce has gone from underdog to a potential (and inevitable) threat to physical retail.

We therefore welcome L'Oréal v eBay's liability standard and consider that even some of its more obvious concerns have been proven groundless as time went by – no litigation thunderstorm was felt over e-commerce ever since 2011 and, ultimately, only *prima facie* liability exemption was cast aside, as the intermediary service provider's liability will still have to be established under general applicable rules (and that is enough of a challenge).

We further understand that L'Oréal v eBay, especially now alongside Stichting Brein v Ziggo, C-610/15, will have significant impact over the role (and eventual liability) intermediary service providers play in respect of the unlawful conduct of its recipients.

Question 1.1.3.

Portugal's regulation of notice-and-take down is exhausted in Decree Law 7/2004, namely in Article 18. The applicable framework, all things considered, makes for very basic regulation.

Article 18 begins by providing that intermediary service providers are not obliged to remove "contents, hyperlinks and analogous processes, or to restrict their access" only because the presumable right holder requests the provider to do so, without prejudice to the fact that said presumable right holder may nevertheless request from the relevant supervisory authority a 'preliminary decision' that shall be awarded within 48 hours and immediately made available to all intervening parties.

Said recourse to the issuing of a 'preliminary decision', however, ended up never being regulated by the Portuguese legislator (with the very own provision making itself contingent on further regulation, as per Article 18(4)). Accordingly, Portugal, in what concerns notice-and-take downs, faces a substantial legal gap in this regard.

However, in the absence of any further regulation, and bearing in mind the general obligations that nonetheless befall over intermediary service providers in accordance with Article 13 of Decree-Law 7/2004, a particularly interesting (and unique) 'self-regulated' effort has made itself noticed in Portugal. This effort, although ultimately not representing a formal notice-and-take down mechanism,

and despite being limited to copyright breaches, may be read as allowing for a procedure that is materially equivalent to notice-and-take down copyright enforcement methods.

We refer to the 30 July 2015 Memorandum of Understanding signed by the General Inspectorate for Cultural Activities ('IGAC'), the Portuguese Association of Telecommunication Operators ('APRITEL'), the Civic Movement Against Online Piracy ('MAPINET' – a group representing several copyright holders in Portugal) and the DNS.PT Association (that is in charge of registrations in the .pt top-level domain, among others,

In accordance with the Memorandum, all websites (i) holding more than 500 unauthorised copyrighted works; as well as (ii) all websites whose repositories are made up of more than 2/3 of unauthorised copyrighted material may be subjected to a DNS block, to be enacted by all Portuguese ISPs. Additionally, websites may be blocked even if they do not fulfil the aforementioned requirements should they provide access to 'particularly damaging content' (e.g., leaks, content facing authorship disputes, etc.).

The list of domains whose blocking is to be requested shall be provided for by MAPINET, alongside evidence of ongoing copyright infringement as well as evidence that MAPINET is effectively acting as an authorised proxy of the copyright holders, to IGAC. IGAC, in its turn, shall verify the information provided and subsequently notify ISPs of a decision to block said websites.

As of the date of writing, 1269 websites are currently blocked by Portuguese ISPs. This list includes pretty much all large-scale national and international websites that are/were popular unauthorised sources of copyrighted content in Portugal.

There are, however, several concerns and drawbacks to this 'para-notice-and-take down approach' that was introduced in Portugal back in 2015.

The first one is quite clear: in the absence of any further regulation on the subject-matter of Article 18 of Decree-Law 7/2004, there is no general legal framework for note-and-take down mechanisms in Portugal. This means that the solution that rose out of the 30 July 2015 Memorandum of Understanding is limited to copyright and connected rights alone. No other fast-paced, purpose-made cautionary mechanism is available for taking down hate speech, online extortion and other illegal contents online – that is still the realm of injunctions and regular legal actions.

Moreover, and perhaps more importantly, there are also significant due process and legitimacy concerns about the Memorandum of Understanding. The Memorandum of Understanding was created on an ad-hoc basis and there is no judicial supervision over the blocking of domains. In addition, IGAC has reportedly ordered the blocking of domains that were hosting lawful conduct because

of misspells at the time of identification of the domains concerned. This situation was apparently fixed on short notice.[2]

Finally, the very own technical solution used for blocking domains is fragile, at best. It works by means of a DNS blocking to outgoing requests and it can be easily evaded by using publicly-available DNS that supersedes that that is provided by ISPs to their customers. Any basic-to-intermediate user can easily change its settings within 5 minutes and gain access to websites blocked by IGAC, with no restrictions. It is, as Google's Eric Schmidt once put it, a "very simple solution to complex problems" that may ultimately backfire for all parties involved.[3]

Our opinion is that the Memorandum of Understanding, as it is, is an interesting – and welcomed – way of overcoming the absence of regulation on notice-and-take downs in Portugal. But it has its limitations. We therefore submit that the best course of action will necessarily involve further regulation on this matter, thus tackling the reason for why the very own Memorandum of Understanding came to be. The mechanism foreseen in Article 18 of Decree-Law no. 7/2004 shall be put in motion, by means of concrete regulation, and due diligence over which websites shall be blocked must be exercised. In addition, a solid appeals system – as well as an expedite mechanism of judicial supervision – shall be put in place and the scope of notice-and-take down mechanisms, in whichever form, shall extend beyond copyright enforcement. Finally, and not withstanding evident technological challenges, other more effective, non-DNS Blocking-based mechanisms shall be designed insofar there is sufficient control and accountability over their use.

Question 1.1.4.

Portuguese courts would have faced the same difficulties Belgian courts did when considering injunctions based on grounds similar to those that led to Scarlet v SABAM and SABAM v Netlog.

The legislative background behind both cases is essentially similar to that that also applies in Portugal. As mentioned before, the E-Commerce Directive was transposed in Portugal by means of Decree-Law 7/2004. In doing so, the Portuguese legislator expressly provided that no general monitoring obligation should be borne by service providers. This would mean that, in principle, when granting injunctions, national courts should ensure that their injunctions do not give rise to a 'general monitoring obligation'.

However, in both Scarlet v SABAM and SABAM v Netlog, the CJEU seems to have suggested that specific blocking requests, that are effective thereafter

[2] See https://shifter.pt/2016/01/foi-bloqueado-o-primeiro-site-nao-pirata-em-portugal/ (in Portuguese)
[3] See https://www.theguardian.com/technology/2011/may/18/google-eric-schmidt-piracy

and that do involve a seemingly mitigated general monitoring obligation, do not necessarily go against what is prescribed in the E-Commerce Directive.

As Curia's media release on Scarlet v SABAM read, "*The Court's reply is that EU law precludes an injunction made against an internet service provider requiring it to install a system for filtering all electronic communications passing via its services which applies indiscriminately to all its customers, as a preventive measure, exclusively at its expense, and for an unlimited period*". In theory, this suggests that *some* injunctions – although none of those that require measures with cumulative characteristics such as those find above – may comply with EU law, even if they do imply some sort of (mitigated) general monitoring obligation.

Recently, in 2017, the Portuguese Intellectual Property Court (a unique IP competence Court at national level) issued an injunction[4] in line with strict measures to prevent and stop the violation of IP rights spread online through a social networking service. The claim has been presented by a Portuguese Public Institute against unknown parties using its logo on TWITTER without the Claimant's authorization, using it either for wrong information or with insulting statements. The Claimant alleged that given it is an earnest public institution linked to education, with a reputation that must be defended, such inappropriate use impairs that reputation, calling into question the truthfulness of its information and the reputation that it wishes to keep.

The court decided to forbid the defendants from using such logo which is owned by the Claimant without the Claimant's authorization. At the same time the Court, at the Claimants request, ordered that TWITTER to be notified to withdraw from its messaging service all uses of the Claimant's mentioned logo that exist and are published in it. It has also been ordered to TWITTER to put in place all appropriate measures to stop and block access to the service provided by TWITTER of addresses that use the Claimant's abovementioned logo and that are not of the claimant itself.

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.

The Consumer Sales and Guarantees Directive has been implemented in Portugal by Decree-Law no. 67/2003, of 8 April, subsequently amended by Decree-Law no. 84/2008, of 21 May which introduced certain additional provisions clarifying the application of the guarantees regime to the sales of immoveable (real estate) goods. A review of judicial decisions issued in disputes concerning rights

[4] At the time this text is being written the main file is still pending.

invoked under this legal regime reveals that some issues have been repeatedly raised regarding remedies claimed by consumers.

These include questions on determining conformity of goods sold as Portuguese law has introduced a presumption of non-conformity in certain circumstances where the goods sold do not conform to objective, general, criteria rather than to contract specifications or pre-contractual information given by the seller. In these cases, determining what is the *normal quality and performance* of goods of the same type may not always be obvious and will require adducing concrete facts to support the presumption of non-conformity.

Another major issue has been determining whether consumers' rights may have lapsed by the time they initiate legal proceedings and how to assess the applicable time limits in actual cases. The issue of whether notification of defects by the consumer to the seller is made within the time limits has generated significant discussion in quite a few cases, with sellers frequently arguing that the rights asserted against them have already lapsed due to untimely notification. The summons of a seller following initiation of judicial proceedings by a consumer has already been deemed by the Supreme Court as an adequate means to give notification of no conformity, if it is effected within the two-year (for moveable goods) or five-year (for immoveable, real estate, assets) guarantee periods.

Question 1.2.2.

The proposed Directive appears to provide for appropriate rules bearing in mind the specific characteristics of digital content, its technical complexity and often intangible nature. The economic importance of activities related to digital content and the fact it can be easily, and in many cases instantaneously, purchased or accessed online by users, justify the Commission's option (reflected in Article 4) in favour of full harmonisation of the rules on digital content as the corresponding demand is growing in all Member States and a uniform set of rules will enable producers of digital content to ensure compliance throughout the EU at significantly lower costs whereas consumers will benefit from greater legal certainty.

Some aspects of the proposed Directive on digital content represent a positive effort to formulate rules that are technologically neutral and as future-proof as possible (e.g. the broad definition of digital content in Article 2(1)) whilst acknowledging that the supply of digital content has some unique features which require, for example, that interoperability with the user's devices and software be addressed when assessing conformity of the content with the contract. Other provisions may prove difficult to enforce in practice, such as the duty laid out in Article 13(2)(b) for the supplier to take all measures to avoid the use of counter-performance other than money (i.e. consumer data) following termination of the contract by the consumer.

Three innovative aspects stand out. Firstly, Article 9(1) states it is for the supplier to demonstrate conformity of content it which provides; this reversal of the burden of proof is reasonable given the technical difficulties consumers would face in demonstrating, or even detecting, the reasons for a lack of conformity, and Article 7 provides an additional safety valve for suppliers in the event of faulty integration. Secondly, by making express reference to the need for content to be free of any third party IP rights (Article 8) in order to prevent a legal defect resulting in non-conformity, the proposal should greatly minimise copyright infringement issues which are a major concern in the distribution of and access to digital content. Thirdly, Article 16 effectively outlaws binding loyalty clauses of more than 12 months in contracts for the provision of digital content by guaranteeing the consumer's right to terminate at any time following expiry of that period.

On a related note, ANACOM has recently (November 2017) issued a recommendation[5] to electronic communications operators following a significant number of complaints by mobile internet users on the billing of allegedly unsolicited content-related WAP services (e.g. ringtones, games, wallpapers). The recommendation is for operators to only bill for these services once users have expressly and specifically authorised payment for each of the contents/services by means of a durable format.

Question 1.2.3.

This proposed Directive also appears to provide for generally appropriate rules in light of its stated goal of removing contract law barriers to online trade and fully harmonising key consumer contractual rights.

Under the proposal, consumer rights are to be significantly strengthened in several respects. Determining the conformity of goods sold must take into account not only what was promised in the contract terms but also several subjective and objective criteria and incorrect installation of the goods will be deemed to constitute lack of conformity where the installation belongs to the seller's sphere of responsibilities. The reversed burden of proof for the absence of lack of conformity at the time of delivery will be extended to a period of 2 years. In addition, consumers: (i) may not be required by national laws to notify the seller of any defects, regardless of the corresponding deadlines; and (ii) must be entitled to a price reduction or to terminate the contract in situations where the seller does not repair the lack of conformity, or replace the goods purchased, within a reasonable time, even if the lack of conformity is minor.

Despite its general appropriateness in the context of online sales, this proposal risks creating two levels of protection for equivalent sale of goods transactions

[5] https://www.anacom.pt/render.jsp?contentId=1421457

depending on whether the goods are sold online or offline (according to Article 19, Directive 1999/44/EC will have its scope amended and limited to transactions which are not distance sales contracts). This may in effect make compliance more costly and complex for sellers who operate a multichannel distribution network, with traditional brick-and-mortar retail outlets alongside e-commerce platforms. Arguably, online sales will face a heavier regulatory burden with specific consumer protection rules than traditional retail of the same goods.

Question 1.2.4.
Both the proposed Directives referred to above (digital content and online and other distance sales of goods) have opted for a full harmonisation approach based on the definition of a minimum set of identical rules and an equivalent level of consumer protection in all Member States. As such, they should contribute to minimise some of the problems that currently undermine consumer protection cooperation mechanisms in the EU (e.g. traders guilty of cross-border infringements to consumer protection rules will no longer be able to evade enforcement by merely relocating to another Member State in order to benefit from more relaxed consumer protection regimes). Both Directives are to be added to the list of relevant instruments contained in the Annex to Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. In parallel, the Commission has approved a proposal for a revised regulation on consumer protection cooperation[6] which should further contribute to effective enforcement of widespread infringements or intra-Union infringements and strengthen surveillance, alert and mutual assistance mechanisms between the competent national authorities.

Question 1.2.5.
The above instruments of EU consumer protection law already deal extensively with the main aspects that may impact on a consumer's dealings with any trader, including online sellers. The Unfair Commercial Practices Directive prohibits any unfair commercial practices, including misleading actions or omissions intended or likely to deceive consumers and aggressive commercial practices, and contains an extensive listing of types of practices which are considered unfair in any circumstances. The Unfair Contract Terms Directive introduces a general requirement of good faith that seeks to prevent significant imbalances between the rights and obligations of consumers vis-à-vis sellers and suppliers (under the corresponding legal regime in Portuguese law several unfair contract terms used by online providers have been deemed abusive and prohibited – see 1.2.6). And the

[6] COM(2016) 283 final.

Consumer Rights Directive has fully regulated aspects such as pre-contractual information to be provided to consumers, their right of (free) withdrawal in the initial stages after concluding a contract and rules on delivery conditions. These directives already protect consumers in their dealings with online platforms. Nevertheless, the fact that they have not fully harmonised national law rules on the aspects they cover has left some degree for legal fragmentation and for differing levels of protection according to each Member State. This has the potential to inhibit cross-border trade in particular regarding online sales (which are by far the main channel for distance purchases) as consumers are unsure as to exactly what rights they possess and how to exercise them depending on what platform they purchase from. In this context, the full harmonisation approach followed by the Commission in its proposals on digital content and online sales of goods seems fully justified and should adequately supplement the protection to consumers already resulting from the directives above.

Question 1.2.6.
Under the rules on standard contract terms (Decree-Law no. 446/85, of 25 October), which consumers have no possibility of negotiating, a relevant number of inhibitory actions have been brought challenging the validity of online providers' standard terms and conditions as being unfair (abusive) and seeking their prohibition. Several types of unfair clauses have been prohibited, including provisions governing the return of goods in distance contracts, liability limitations or exclusions, delivery terms and post-sales assistance to technical equipment. Traders who have been subject to these actions include online providers of consultancy services, travel and lifestyle products and retail distribution (catalogue sales). Relevant decisions, starting 2015, are published in a registry maintained by the Directorate-General for Justice Policy (DGPJ) which is available for consultation at: http://www.dgpj.mj.pt/DGPJ/sections/sobre-dgpj/anexos/registo-das-clausulas/

Question 1.2.7.
No. There do not appear to be any valid reasons why the scope of consumer protection rules should be extended to businesses and SMEs. Small and micro-businesses periodically purchase goods and services in the course of their own commercial or professional activities, or for resale, and do not warrant the same degree of protection as that which applies to consumers in B2C transactions (it is difficult to argue that any business, even an SME, is by definition a weaker party in a supply relationship). This was also the view of a majority of respondents, including consumer associations, in the context of the stakeholder consultations that preceded the proposed Directives on the supply of digital content and online and other distance sales of goods.

1.3. Geo Blocking

Question 1.3.1.

Under Regulation 1215/2012, as previously under Regulation 44/2001, in disputes arising from consumer contracts consumers are assured the benefit of opting either to sue a trader in the courts of the Member State where they are domiciled or in the courts of the Member State where the trader is domiciled (conversely, proceedings may only be brought against consumers in their own Member State). This safeguard depends, notably, on whether the trader directs commercial or professional activities to the Member State where the consumer is domiciled, condition which has been interpreted by the Court of Justice as requiring more than just having an internationally accessible website.

In joined cases C-585/08 and C-144/09, *Pammer* and *Hotel Alpenhof*, on the interpretation of Article 15(1)(c) and (3) of Regulation 44/2001, the ECJ held that determining if a trader is directing its activities to consumers in a Member State other than that of its establishment will depend on "evidence demonstrating that the trader was envisaging doing business with consumers domiciled in other Member States, including the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with those consumers" (§76). Relevant evidence may include, in addition to direct statements by the trader to the effect it is offering goods or services in one or more designated Member States, indirect factors such as: the international nature of the activity pursued; mention of telephone numbers with an international code; use of a top-level domain name other than that in which the trader is established or use of neutral top-level domain names such as '.com' or '.eu'; description of itineraries from one or more other Member States to the location where the service is provided; mention of an international clientele; or if the trader's website permits consumers to use a different language or currency to those of the trader's Member State of establishment (§§ 83, 84). In *Mühlleitner*, the Court added that factors such as the establishment of contacts or reservation of goods or services at a distance, or, *a fortiori*, the conclusion of a consumer contract at a distance, are indications of a connection between the contract and the trader's activity (case C-190/11, § 44).

In a sense, the test on "directing activities" to the Member State of the consumer's domicile rests on the degree to which a trader proactively seeks to advertise and promote its goods and services in more than its own Member State of establishment and, as such, to facilitate access by consumers residing in multiple Member States by designing its commercial activities with a wider territorial reach. In turn, the proposed geo-blocking Regulation seeks to prevent discrimination of customers (not merely consumers but also undertakings) based on geo-factors, such as nationality, place of residence or place of establishment, regardless of the format and scope with which the trader has designed its activities.

The geo-blocking Regulation will prevent traders from applying different (discriminatory) conditions of sale to consumers from different Member States in three situations set out in Article 4(1): sale of goods without physical delivery; sale of electronically supplied services; and the sale of services provided in a specific physical location. It will also prevent them from, based on the same reasons, blocking access to their websites or rerouting customers to different country versions of a website without their consent.

Although in practice compliance by traders with these obligations under the geo-blocking Regulation will sometimes coincide with factors evidencing that they direct their activities to the Member State of a consumer's domicile, under Regulation 1215/2012, each set of rules pursues different goals. The geo-blocking regulation focuses, notably, on the general conditions of sale made available by traders prior to conclusion of a contract whereas Regulation 1215/2012 relies on the test of "directing commercial activities" for jurisdictional purposes in order to ensure a more beneficial regime for consumers regarding contracts they have concluded (irrespective of their substantive terms). Furthermore, the subjective scope also differs as Regulation 1215/2012 specifies a protective jurisdictional regime for the benefit of consumers only whereas the geo-blocking Regulation extends the guarantee of non-discriminatory trading conditions to any "customers", including undertakings. Understandably, Article 1(5) of the geo-blocking Regulation expressly provides that compliance with its rules "shall not be construed as implying that a trader directs his or her activities to the Member State where the consumer has the habitual residence or domicile" within the meaning of point (c) of Article 17(1) of Regulation (EU) 1215/2012.

1.4. Questions related to the collaborative economy

Question 1.4.1

Several collaborative economy businesses have been increasing their activities in Portugal which has, predictably, generated a defensive reaction from traditional service providers.

The introduction of Uber services in Portugal, in 2014, sparked a lively debate on the regulation of passenger transport services (with a driver) and on the requirements that this type of service should be subject to in the event it is mediated by an online platform. In 2015, the Portuguese Taxi Association ("Antral") filed a legal action against Uber seeking an *ex parte* injunction to prevent the company from operating in Portugal. The injunction was granted by the first instance court and recently confirmed on appeal by the Lisbon Court of Appeals. A further appeal may lie to the Constitutional Court on constitutional issues and, in any case, serious question marks remain as to its practical effects and enforceability given that the injunction does not cover the corporate entity in the Uber

group which actually provides services in Portugal. In the meantime, the Portuguese Government has initiated a review of the regulatory framework, since it remains unclear exactly what requirements would be adequate for the provision of services by collaborative platform operators.

The short-term rental market has also been showing exponential growth, with the proliferation of Airbnb-listed houses in the main Portuguese cities leading to discussions on whether this business model should be restricted or controlled. A contentious issue, raised by recalcitrant neighbours, has been that of determining whether the provision of short-term rental services by an apartment owner, for instance, should be subject to authorisation by the building's condominium general meeting. In particular, the argument has been raised that providing short-term rental services (to the extent this constitutes a trading or commercial activity) is contrary to the residential uses provided for by urban buildings' horizontal property regulations and to each apartment's license for use (limited to residential purposes). Although, to our knowledge, Airbnb business operations have not been specifically targeted, the Lisbon Court of Appeal has already decided that the condominium general meeting must approve the conversion of residential apartments to a short-term rental business for tourists. However, this understanding was reversed by the Supreme Court in March 2017 on the grounds that even though a short-term lease, against payment by the user, may constitute an act of trade, this does not mean that a commercial activity is carried out within the leased unit as this is only made available, precisely, for residential, or accommodation, purposes.

Question 1.4.2.

Collaborative economy businesses face serious hurdles related to market access. Since they quickly become popular, this type of services has a relevant impact on traditional players. In the passenger transport sector, in particular, taxi operators complain that they must comply with stricter regulatory and licensing requirements (including quantitative restrictions on access to the market and regulated prices) which put them at a disadvantage vis-à-vis online platform operators, since the same requirements do not apply to the latter.

In December 2016, following a public consultation, the Portuguese Competition Authority ('AdC') published an extensive report on competition and regulation in passenger transport services[7] analysing the constraints that existing rules pose to competition in this market. Limitations such as quantitative restrictions on the number of operators or the administrative setting of prices (taxi tariffs are

[7] Press release available at http://www.concorrencia.pt/vEN/News_Events/Comunicados/Pages/PressRelease_2016.aspx?lst=1&Cat=2016.

set by conventions between the Directorate-General for Economic Activities and associations representing the taxi license holders) were heavily criticised by the AdC for being disproportionate and harmful to competition. As a result, the AdC recommended that the Government reassess the current quantitative restrictions and price setting regulations for taxis, with the explicit recommendation that the new rules should not extend heavy regulation to new entrants but merely establish a level playing field. The debate on regulatory reform is still ongoing.

Question 1.4.3.

The main activities in the collaborative economy in respect of which market access and licensing requirements have been the focus of discussion in Portugal are related to online platforms enabling passenger transportation services and short-term rentals for tourist accommodation.

In respect of passenger transportation services enabled by online applications, a great deal of uncertainty remains as to what market access requirements and procedures apply and, in particular, whether it is reasonable to subject this type of services to the same requirements as those applying to traditional taxi services, which are essentially contained in Decree-Law no. 251/98, of 11 August (as amended). Taxis are subject, *inter alia*, to: (i) issuance of a permit by the IMT (Institute for Mobility and Transportation), which may not be transferred and has a maximum term of 5 years; (ii) issuance of a municipal taxi license for each vehicle; (iii) quantitative restrictions, set by each municipality for at least 2-year periods, on the maximum number of taxis that may operate within each municipality.

A legislative proposal (50/XIII) by the Government was submitted to Parliament in January 2017 aiming to create a specific legal regime for "individual paid passenger transportation services in unmarked vehicles" and for online platforms enabling these services. This proposal sought to clearly distinguish transportation services offered over collaborative platforms from traditional taxi services, the former being explicitly qualified as information society services. Under this proposal, both the transportation service operators and the online platforms mediating between them and end-users would be subject only to a prior notice to the IMT. Additional conditions regarding vehicle maintenance, driver suitability and training would apply and prices would be set freely, in accordance with tariff levels or calculation formulas displayed by the platform. This proposal is still under discussion and has not been enacted.

In the case of short-term rentals, in which most residential properties on offer are made available through online platforms, the basic rules governing access to this activity are set out in Decree-Law no. 128/2014, of 29 August, which approved the legal regime on the management of short-term rental establishments. These are defined as those offering "temporary accommodation services to tourists,

for consideration, and satisfy the requirements" set out in this statute, whether accommodation is made available by physical or legal persons. Management of a short-term rental establishment is presumed to exist, *inter alia*, when an apartment or building is advertised for tourist lodging or temporary accommodation on an online platform or website.

Essentially, short-term rental providers must: a) register with the relevant municipality in their territorial area and; b) comply with sanitation and safety requirements, including fire hazard regulations. Access requirements and procedures are quite clear and transparent and registration involves a mere prior notice in an electronic platform (which must be accompanied by supporting information and documents). In addition, certain conditions specified in Administrative Order no. 83/2016, of 4 August, must be complied with, including the use of outdoor identification plates, making available a complaints book and keeping a monthly register of the number of guests.

Question 1.4.4.
In the context of collaborative economy activities, there is little visibility as to the degree or intensity of consumer complaints so far. According to the Portuguese Consumer Protection Association (DECO), although the level of complaints is still low, issues such as lack of information, non-conformity of rental properties with their online descriptions and limitations regarding protection of users' personal data have been reported.

Question 1.4.5.
According to the general definition on the scope of consumer protection rules contained in the legal regime for consumer protection (approved by Law no. 24/96, of 31 July, as amended) for a peer-to-peer provider of an underlying service to qualify as a trader it must carry out this activity in a professional capacity. Only in that case will its counterparty qualify as a consumer, as results from Article 2(1) of this statute: "A consumer is considered to be any person to whom goods are supplied, services are rendered or rights are conveyed, for non-professional use, by a person *carrying out in a professional manner an economic activity* for the obtainment of benefits." This definition fits with the definitions of a trader under Directive 2011/83/EU, for instance, or under the Unfair Commercial Practices Directive, which relies on this person's activities being carried out for purposes relating to his trade, business, craft or profession. Portuguese law does not specify when a peer-to-peer provider of an underlying service should qualify as a trader which must be assessed on a case-by-case basis. This may involve factors such as the regularity with which a person provides services or sells goods on P2P platforms (excluding merely occasional offers), revenue thresholds or what proportion of that provider's overall income is derived from these activities.

Question 1.4.6.
It is uncertain whether eventual lack of consumer confidence in peer-to-peer services requires the adoption of specific legal rules in respect of the underlying services. Consumers are generally aware that, given the flexibility and informal nature of most business models in the collaborative economy, transacting over a P2P platform may often involve a greater risk regarding the quality or fitness for purpose of the goods or services involved and may be willing to accept that risk in exchange for the advantage of lower prices or being able to purchase through sharing models. This conclusion is supported by the key findings in the exploratory study of consumer issues in online peer-to-peer platform markets published by the Commission in May 2017[8], according to which only 16% of consumers completely agreed to feeling safer or more protected when buying, renting or hiring through conventional businesses. Furthermore, the horizontal nature inherent in a peer-to-peer model (where consumer-to-consumer transactions proliferate) differs markedly from the usual "vertical" relationship between traders and consumers and in this context it may be excessive to impose specific regulation on a multitude of non-professional, mostly occasional, providers (e.g. sellers and buyers will tend to be affected by equivalent information asymmetries).

Online rating and review mechanisms are undoubtedly a useful tool to reinforce trust although, in the case of underlying service providers, this will only be effective for regular (professional) providers, who offer goods or services on multiple occasions and may, therefore, be properly rated on a minimum volume of transactions. Regarding the actual peer-to-peer platforms, accreditation mechanisms and voluntary codes of conduct may provide an additional level of safety and trust. In Portugal, the Portuguese Consumer Protection Association (DECO), together with the Digital Economy Association (ACEPI) and the DNS.PT association, have designed an accreditation mechanism that online e-commerce platforms in general may sign up to in order to benefit from a quality certification under the Confio ("Trust") stamp. They have also approved a voluntary code of conduct (Confio.pt), in accordance with Article 16 of the e-Commerce Directive, which is available at https://www.confio.pt/o-confio/codigo-de-conduta/.

2. Digital media

Question 2.1.
We have no knowledge of any national case law regarding this particular provision of the AVMS Directive and or audio-visual material offered by online newspapers.

[8] http://ec.europa.eu/newsroom/just/item-detail.cfm?&item_id=77704.

Question 2.2.
We consider that the legislative proposal to which the question refers is a step in the right direction. As regards the extension of the scope of application towards video platforms, we find that it should also cover rules on commercial communications. Portuguese law does not set out sector-specific rules for audio-visual platforms such as Youtube; however, the Law of Television establishes a legal frame-work for on-demand audio-visual services.

Question 2.3.
We have no knowledge of any disputes concerning the application of the country-of-origin principle with regard to audio-visual media service providers established in other Member States our outside the EU.

Question 2.4.
The introduction of independence requirements for media regulators at EU would, from our standpoint, be a step forward and would contribute to the creation of a single market for audio-visual media services. We are not aware of any obstacles in Portuguese law to independence requirements for media regulators; on the contrary: under Portuguese law, there are strict rules with respect to the independence of media regulators. As regards problems of undue political and or commercial pressure on media regulators in Portugal, some news arise from time to time. Yet, we are not aware of any law suits on this matter.

Question 2.5.
All the areas exemplified in the question (product placement or sponsoring; unsuitable content for minors on television; dissemination of hate speech; role of public service broadcasters; and growing media concentration) have, from time to time, been discussed in the public debate and or given cause to complaints by viewers / consumers addressed at media companies. In addition, a recent case of media concentration has been analysed (in a non-binding manner) by the Portuguese telecommunications regulator.

Question 2.6.
We are not aware of any initiatives such as those described in the question. For the time being, we do not think that an EU-wide harmonised approach is necessary.

Question 2.7.
The specific regime for copyright licencing for TV and radio broadcasting by satellite, as it results from Directive 93/83/EEC (that was transposed in Portugal by Decree-Law 333/97, of 27 November), remains relevant in Portugal, in the sense

that that regulation is still the applicable law. The Portuguese legislator, in transposing Directive 93/83/EEC, went beyond its original scope and added rules on the governing jurisdiction for disputes related to lack of authorisations by the respective right holders for retransmissions by cable. That being said, Decree-Law 333/97 was not amended ever since its entry into force in 1997.

Furthermore, and to the best of our knowledge, no Portuguese court has ever discussed the extension of the rights found in Decree-Law 333/97 to online transmissions of broadcasting organisations, nor are we are aware of any (national) discussion regarding its extension to said online transmissions.[9]

Question 2.8.

The main barriers in Portugal to cross-border portability of digital content are pretty much the same barriers that European consumers face in other Member States, meaning blocks to content and/or content that, upon being accessed, differs from the content that is made available in the respective country of residence.

However, we understand that, in what concerns Portuguese and Portuguese consumers, these barriers are made relatively more significant due to the country's peripheral position within the EU digital content market and due to Portugal's relatively smaller domestic market.

In addition, Portugal, unlike many other Member States, does not share its language with any other European country – and, unlike the situation in Denmark, Sweden and Norway (the 'Scandinavian language cluster'), language barriers and tastes in Portugal and Spain differ enough so as not to allow a one-sized approach by content providers. Thus, licensing agreements are often made separately and, more often than not, those agreements go hand-in-hand with separate localisation efforts by the respective service providers.

As a result, content that is available in Spain is often not available in Portugal – and vice-versa (although, naturally, due to different market sizes, the former occurs a lot more frequently than the latter).

Additionally, and especially in what concerns online video streams, when it is indeed possible to gain access to the same digital content across the border, localised versions of that content are often forced on customers. This means that, should a paying Portuguese consumer cross the border into Spain and be able to access the same film or TV series he/she pays for backing in Portugal, and that is also available in Spain, he/she will not have access to Portuguese subtitles and/or dubs (if applicable).

[9] In addition, the limited number Portuguese literature available on this matter mainly relates to the European Commission's consultation review of Directive 93/83/EEC and to the proposal for a regulation on ensuring the cross-border portability of online content services in the internal market.

Coincidently, and notwithstanding the fact that this much is also applicable to all other EU countries, because Portugal's only border is with Spain and because both countries exchange very significant tourism flows[10], it is not particularly surprising that cross-border portability is a significant nuisance for border-crossing Portuguese consumer. Unlike other EU consumers (e.g. Danish residents visiting Sweden or Belgians residents visiting France), Portuguese residents find a particularly adverse situation regardless of where they go, and even in their only neighbouring country.

In fact, this much is clear from the EC's Consumer Survey on cross-borders obstacles to the Digital Single Marketing, where (traveling) Portugal-based consumers constantly ranked as one of the surveyed groups that most often faced difficulties in accessing streamed online content when traveling.[11]

Ideally, these barriers should be tackled Europe-wide within the DSM strategy, thus allowing for full harmonisation of applicable rules and market access. Indeed, a fragmented legal framework on local licensing matters is what brought us here in the first place and, accordingly, the situation must be solved on a top-to-bottom basis. This is the reason why we definitely welcome Regulation (EU) 2017/1128.

The new Regulation effectively means that the monitoring of the country of residence of the consumer will cease to exist as it is today. We further understand that Regulation (EU) 2017/1128 is quite clear in relation to the (desirably) minimal role the verification of the Member State of residence shall play in the relationship at hand.

Indeed, the Regulation provides that the monitoring of the Member State of residence shall be undertaken by means of no more than two of the elements referred to in Article 1(1) and it shall be "reasonable, proportional and effective". Furthermore, in accordance with Article 8, and in is essentially a throwback to the GDPR, the use of any means to assess a country of residence shall be "limited to what is necessary and proportionate in order to achieve this purpose".

Therefore, in light of the fact that, as we interpret Article 5 of Regulation (EU) 2017/1128, service providers do not have the right – nor the obligation – to control the country of residence 'on a regular basis', and, as general rule, should

[10] Around 2 million Portuguese – out of a population of 10 million – visited Spain in 2016, and Spain has constantly ranked as the top country of origin of tourists visiting Portugal for the past 5 years. See http://rr.sapo.pt/noticia/44995/portugal_atrai_mais_turistas_espanhois_com_qualidade_e_diversidade_de_oferta *(in Portuguese)* and https://elpais.com/elpais/2017/01/31/media/1485886612_898631.html *(in Spanish)*.

[11] European Commission, Consumer survey identifying the main cross-border obstacles to the DSM and where they matter most, forthcoming 2015 – only 16% of Portuguese residents reported as being able to stream films and TV series while in another EU-country.

only do so "*at the conclusion and upon renewal of a contract*"[12], we understand any regular control of the country of residence, except where the provider "*has reasonable doubts about the subscriber's Member State of residence during the course of duration of the contract*"[13] will be unlawful, as it is not "*necessary*" nor "proportionate in order to achieve [the] purpose"[14] of Article 5.

3. Digital infrastructures

Question 3.1.

In Portugal, no formal rules on net neutrality existed prior to the adoption of Regulation (EU) 2015/2010. However, the matter in analysis was subject to two bills (418/XI/2ª, from September 30, 2010, and 103/XII/1ª, from December 3, 2011). Despite the intention to adopt the principle of net neutrality, no formal rule was approved on the matter. The only reference to this principle came with the transposition of Directive 2002/22/CE to the Portuguese legal order, with article 27, nr.1 point c) stating, in a generic way, the terms established in the above mentioned Directive[15].

In any event, the subject of net neutrality has been discussed prior to and after the adoption of this Regulation, both in the context of the civil society, events and conferences hosted by ANACOM (the country's regulator for the telecommunications sector) and in the political arena. In particular, the net neutrality subject was formally discussed in Portugal following the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions regarding "*the open internet and net neutrality in Europe*", dated April 19th, 2011.

In what concerns the practices of zero-rating, ANACOM has included the analysis and monitoring of this matter in its 2018-2020 action plan, in which ANACOM notes that it will continue to pay attention to aspects related to consumer protection, particularly those connected with the implementation of the regulation over open internet and connected to new offers by IPSs and OTT pro-

[12] See Article 5 (1) of Regulation (EU) 2017/1128.

[13] See Article 5(2) of Regulation (EU) 2017/1128.

[14] See Article 8(1) of Regulation (EU) 2017/1128.

[15] Article 27, nr.1 that "Without prejudice to other conditions provided for in general law, undertakings providing publicly available electronic communications networks and services may be subject in the exercise of their activity to the following conditions" (...) c) Transparency obligations on operators of public communications networks providing electronic communications services available to the public to ensure end-to-end connectivity, in conformity with the objectives and principles set out in article 5, disclosure regarding any conditions limiting access to and/or use of services and applications where such conditions are allowed in conformity with the law, and, where necessary and proportionate, access by the NRA to such information needed to verify the accuracy of such disclosure".

viders – including evaluation of zero rating and traffic management practices, among other related topics.

ANACOM has stated in the Report on the application of articles nr. 3 and 4 of Regulation (EU) 2015/2020 (April 2016-2017) that it is important to take into consideration the principles stated on the "BEREC Guidelines on the implementation by National Regulators of European Net Neutrality Rules", approved on August 30th, 2016.

In order to properly follow such Guidelines, ANACOM requested, in 2016, that the major Internet Service Providers ("ISP") – MEO, NOS and Vodafone – complete a survey on the zero-ratings subject, in order to acknowledge the existence (and consequent extension) of zero-ratings practices in Portugal.

ANACOM does not state, in such Report, which practices should or not be prohibited, stating only that the evaluation should be made on a case-by-case basis, and always taking into consideration the above mentioned BEREC Guidelines and any EU decision/recommendation that may be adopted in the future.

Question 3.2.

The creation of a single market for telecommunications networks or services is one of the main topics of discussion in the telecommunications sector in recent years, particularly considering the approval of Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the EU.

The idea of a pro-European approach on this matter is not new, but took a huge step forward with the Proposal for a Directive of the European Parliament and the Council establishing the European Electronic Communications Code, from September 14th, 2016 ("EECC") which establishes a general authorization mechanism for the provision of electronic communications services and networks, thus not requiring an explicit decision or administrative act by the National Regulatory Authorities ("NRA"). However, if some Member States require a notification by providers of electronic communications networks or services when they start their activities, such notification should be submitted to BEREC, which acts as a contact point and must, if necessary, forward the notifications to the NRA in all Member States in which such providers intend to provide their networks or services.

Taking this into consideration and the fact that the majority of NRAs adopt, in a great extension of their attributions, European Regulations, Directives, Decisions and Recommendations, the natural tendency may be for NRA deci-

sions and positions regarding the provision of telecommunications networks and services to become more similar and closer to each other in the underlying regulatory approach. This could contribute to the creation of a single market, including the introduction of an EU-wide licensing scheme.

However, despite the globalising nature and tendencies of the telecommunications technology and market, there are still cross-national differences in regulatory regimes, as a result of different strategic priorities, national legal outputs and the structural and commercial aspects of the market in each given EU jurisdiction.

This may act as a deterrent for a single telecommunications market in the EU. Moreover, it also important to consider the risk of a single market for telecommunications networks and services bottlenecking the activity of the service providers and jeopardizing the proper operation of NRAs as a result of centralised operations.

Moreover, specific EU initiatives aimed at unifying the EU telecom sector have been met with some opposition. This is the case, for example, of the proposed 25-year spectrum licence, which is now included on the Directive establishing the European Electronic Communications Code. Also the establishment of a pan-European licensing scheme is being met with some opposition, as NRAs are reluctant to give up control on the definition of the conditions associated with spectrum management.

In light of this, we believe that, while pan-European licencing schemes have potential in simplifying procedures and access to the activity, it is necessary to adequately determine the extent of any such licences, their scope and nature (i.e. whether they are mandatory schemes or optional). Any decision in this respect would have to take into account the various outputs of the national NRAs and the multi-faceted aspects of the telecommunications sector in the various EU Member-States.

Question 3.3.

As far as we are aware, there are currently no ongoing legal issues regarding spectrum usage and management in Portugal.

Nevertheless, in the context of its functions as regulator for the sector and as the entity responsible for ensuring the management and monitoring of an adequate and effective use of spectrum in Portugal, ANACOM has adopted strategic plans in what regards spectrum.

Specifically, ANACOM has published its 2016 Strategic Spectrum Plan, in which it identifies the main challenges associated with spectrum management in Portugal. In this context, ANACOM noted that the main priorities in this aspect are (i) the future of the 700 MHz band; (ii) mobile broadband and 5G scenario;

(iii) the timely provision of spectrum for short range communications; (iv) wireless phones and cameras; (v) IoT and M2M communications; (vi) broadband wireless communications, namely for emergency service management.

In this strategic plan, ANACOM set out the following strategic actions regarding spectrum management in Portugal:

Foster the utilization of wireless broadband technologies that allow for high speed data transmission;

Improve mobile network's coverage and capacity, namely in rural and remote areas, as well as allow for the provision of new services and mobile applications;

Develop the appropriate regulatory framework for the implementation of wireless broadband networks, by utilizing the available spectrum, such as the available frequency bands and the spectrum currently allocated for wireless broadband applications, such as in the 700 MHz, 1452-1492 MHz and 3400-3800 MHz frequency bands;Adopt the necessary measures for the provision of a total of 1200 MHz for Terrestrial Electronic Communications Services;

- Foster the growth and innovation on M2M/ IoT applications, namely by identifying and solving technical and regulatory questions;
- Evaluate the medium term needs for spectrum (until 2020) for IMT-Advanced systems, namely for LTE-A (LTE Release 10 and posterior); some of the key characteristics for IMT-Advanced systems are the provision of 100 Mbps in high mobility and 1 Gbps in low mobility, as well as increasing the efficiency of spectrum usage (bit(s(Hz); and
- Evaluate the future needs of spectrum for IMT-2020 for 5G, currently in an investigation phase, for which the first technologies are predicted to be available in 2020, being expected for these systems to reach 10 and, in some cases, 20 Gbps; In this respect it is also under investigation the provision of spectrum above 6 GHz; 5G must be seen in a wider context, involving other systems and infrastructures, such as "backhaul" systems.

ANACOM's main concerns stem directly from general legal and regulatory principles, particularly ensuring effective competition and an efficient use of spectrum, as a scarce resource.

To this effect, ANACOM carries out regular monitoring actions and has the right to ask for information and data from any provider to which rights to use spectrum have been granted. While ANACOM carries out an *ex-ante* analysis of the viability and likely effectiveness of granting a given operator the rights to use spectrum in a specific range (considering the possible use of the frequencies, its current and foreseen technological potential, the existence of other parties interested in a specific range and a possible overall impact on the market).

Ex post action is also possible and may be implemented by ANACOM through a specific administrative process, should ANACOM determine that the conditions associated with the right to use spectrum frequencies have not been complied with – this may include spectrum take-back by ANACOM.

Additionally, ANACOM has carried out several initiatives aimed at understanding the circumstances of the market and the concerns/priorities/potential associated with the various players, in order to better adjust its approach and possible action on the matter.

For example, in 2016 ANACOM conducted a public consultation regarding (i) use/availability of spectrum in the 3400-3800 MHz range. This included specific questions aimed at the desirability and potential of this spectrum range for different technologies, services and contexts. In this public consultation, ANACOM also asked for market feedback on the matter of the flexibility of the terms of use for FWA frequencies held by a major local operator.

Moreover, on 12 January 2017, ANACOM launched an applied research and development study, in the area of engineering, in order to analyse scenarios and alternative models of spectrum management, in particular those involving Licensed Shared Access (LSA) concepts in the 2.3-2.4 GHz band. The aim of this study was to evaluate whether, how and to what extent, existing systems (Program Making and Special Events – PMSE) and mobile systems could coexist in the 2.3-2.4 GHz band, taking into account the particularities of each system.

Question 3.4.

As far as we are aware, there have been no legal proceedings associated with ANACOM's independence.

4. Data in the digital economy

Question 4.1.

As is the case with all other EU State-Members, the various Portuguese stakeholders are adjusting to the upcoming reality of the General Data Protection Regulation (the GDPR).

In what concerns official initiatives towards the GDPR, the Portuguese government has established a Working Group, tasked with adjusting Portuguese legislation to the terms of the GDPR. The Working Group is composed of scholars, members of the Government, high-ranking members of the National Board of Security and of the Governmental System Management Control Centre.

In the context of its activity and attributions, the GDPR Working Group is set to work with all relevant stakeholders towards carrying out the following actions: (i) carrying out a public consultation, to take place until 30th September, 2017; (ii) identify the security rules applicable to the processing of personal data, as

per the rules in the GDPR, and present the various alternatives on institutional architecture required for operating the GDPR; and (iii) submit a law proposal by 31st December 2017.

In light of this, the GDPR Working Group has launched the public consultation on the approval of national legislation referring to the GDPR. This public consultation, which is open for input from both companies and individuals, focuses on the following 7 main topics:

1. *Processing of special categories of personal data (genetic, biometric and health data):* should specific demands be set for the processing of this data? If so, which and in what terms?
2. *Processing of data in an employment context:* should national law set specific regimes aimed at protection the rights and interests of employees in the context of labour relationships? If so, which and in what terms?
3. *Data portability rights:* should special rules be created regarding the transfer of personal data between providers of financial, banking, insurance and telecommunications services? If so, which other areas or sectors or activity should be subject to additional demands and obligations on the matter of data flows?
4. *Consent for processing of minors' personal data:* should minors under the age of 16 be allowed to expressly consent to the processing of their personal data? If so, which age should be considered as baseline: 13, 14, 15?
5. *Right to be forgotten:* should the right to be forgotten be reinforced and subject to additional guaranties in relation to what is set out in article 17 of the GDPR? If so, in which sector would that reinforcement be justified;
6. *Automated individual decision-making, including profiling:* other than the exceptions foreseen in article 22/2 of the GDPR, should other exceptions be included in respect of automated processing (namely through algorithms)? If so, in which situations?
7. *Data Protection Officer:* considering the rules in the GDPR on DPO mission and functions to be performed, would it be adequate, in certain sectors of activity, to consider the possibility of determining the appointment of specific DPOs per sector?

The public consultation is taking its course and developments are expected in the short term, with the analysis of all inputs to the public consultation from interested parties and the developments associated with the tasks entrusted to the Working Group.

Question 4.2.

As the 25th May 2018 deadline becomes a more pressing reality, businesses in Portugal are becoming increasingly aware of the impact and importance of the GDPR and of the differences between the current privacy legal framework and the one arising from this new legal instrument.

Indeed, an increasing number of companies are seeking to implement GDPR compliance programs and determining the strategic, operational and commercial impact of the GDPR on business. To this effect and by way of example, a growing number of companies are proceeding to appoint DPOs, prepare Privacy Impact Assessments for ongoing and planned data processing projects, and analysing the application of Privacy by Default and Privacy by Design Principles in the context of their activity and of the product/service at stake. This has caused a boost in the search for specialised legal services.

Moreover, stakeholders are very receptive to GDPR information, as has been noted through the various conferences, courses, seminars and various events and publications held on the matter of the overall impact of the GDPR, DPO training and awareness courses.

In what concerns the level of awareness to the GDPR by different types of stakeholders, according to a study conducted by KPMG, 65% of organizations[16] in Portugal have a medium-to-high awareness regarding the new obligations and impacts of the GDPR. However, according to this study, with less than a year remaining until the application of the GDPR, a vast majority (85%) claims to have not yet initiated the implementation process.

The public sector, the energy sector, as well as the telecommunications, transport, tourism, electronics and insurance sectors acknowledge that there is a delay regarding the implementation of the new measures arising from the GDPR. The healthcare sector and retail sector appear to have implemented measures according to the requisites of the GDPR, probably due to either regulatory constriction and/or to the fact that these sectors deal with big data and sensitive data on a regular basis. Furthermore, 53% of the inquired organizations predict a high to very high impact arising from implementation of the new measures of the GDPR and 43% claim to have designated a responsible body for the needed adaptations. In sum, in our jurisdiction there has been a gradual approach of businesses to the GDPR.

In Portugal, various entities have already begun the GDPR implementation process and are carrying out GDPR-specific compliance programs in order to review their internal procedures, policies, documents, structural organisation and overall approach to privacy and data protection compliance.

[16] More than 100 organizations of various dimensions and sectors participated in the study, which was published on March 2017.

Initially, this concern was addressed particularly by companies operating in highly-regulated sectors, such as the health and pharmaceutical sector, banking and finance, aviation and insurance sectors.

Companies in regulated sectors and/or in international groups tend to be the earlier adopters of GDPR-compliance initiatives, while small and medium-sized businesses seem to have been less quick to implement GDPR compliance programs.

Indeed, as per recent studies, out of a universe of over 1.600 small and medium-sized companies, only 3% had employed a plan towards ensuring conformity with the GDPR on 25th May, 2018; around 44% of the companies enquired admitted to not having implemented any compliance program, while 14% stated that they had employed said measures solely for specific areas[17].

However, while more robust GDPR-compliance numbers seem to be more prevalent in larger companies and companies within the context of international groups, companies operating in less regulated sectors are becoming increasingly focused on these issues, as the GDPR application comes closer to their horizon.

Question 4.3.

What are the most contentious issues in your country (from a legal viewpoint) in relation to IoT (Internet of Things) / smart cities / Machine-to-machine generated data / automated cars? (Ownership issues? Access and use? Liability in case of harm?) Are there any specific legislative measures or regulatory opinions/decisions in this area? What is the status of the policy debate?

The Portuguese Government has publicly stated its commitment to promote and implement IoT applications, smart cities and automated cars.

The market in Portugal is becoming increasingly aware of the potential of IoT, smart cities, M2M data and other corollaries of the information society. Indeed, these tools are an important asset to various market players (including banks, health and pharmaceutical companies, insurance providers and service sector providers). These entities have been investing on the development of tools and business mechanisms based on these assets and aimed at optimising resources.

Indeed, IoT is generally considered in the Portuguese market to be inevitable and a sign of the times.

An interesting side-note is that these aspects of the digital revolution have contributed to the increasing establishment of start-up tech companies, which are aimed at creating new software, hardware, business strategies and consulting services aimed at these aspects.

[17] September 2017 study by the Institute for support to small and medium companies and investment (IAPMEI) the Association for the Promotion and Development of the Information Society (APDSI) and the Portuguese Association for People Management (APG).

A common concern in this respect is the need to ensure compatibility between technological potential and user privacy/data security. Indeed, not only are data breaches an increasing reality, but the potential damage arising therefrom, particularly in regulated sectors dealing with highly sensitive information, is significant from a legal, financial and reputational point of view.

We also note that IoT may raise data ownership, spectrum, access, use and liability issues from a legal point of view. IoT devices operate as part of an ecosystem, and many of the devices are being designed to communicate with each other. As such, data ownership will continue to be an extremely important issue, as results from the EU public consultation on Building a European Data Economy which occurred between 10th of January to 26th of April 2017. Results will expectedly feed into the Commission's initiatives on data announced in the Mid-term review of the 2015 Digital Single Market strategy and contribute to a common framework on this matter.

In what concerns autonomous vehicles, Portugal is party to the Convention on Road Traffic, which permits the circulation of autonomous vehicles but not of vehicles without a driver (including one who is operating the vehicle from outside) due to the issue of control. From a legislative standpoint, the circulation of motorized vehicles on public roads depends on the existence of a human driver, placed inside the vehicle. The Government is presently pursuing the creation of tech-free zones as publicized in the 2017 state budget. As such, the main issues enunciated in the question are still being evaluated and the legal framework may be broadened and adapted to dissolve the present lack of clarification.

Question 4.4.

Although the legal right to be forgotten is not currently expressly foreseen as an independent principle in Portuguese law, it could already be taken to constitute a result of the data subject's right to object to the processing of his/her personal data, as well as the general principle that personal data may only be processed for the period of time during which it is necessary.

In practice, considering the legal emphasis on data subject protection and on the safeguard of the data subject's rights, the data subject's right to having his/her data deleted would possibly prevail over the legitimate interests of the data controller, whenever a substantially legitimate interest was not at stake. For example, data processed by employers for the purpose of managing whistleblowing programs, data pertaining to public figures in a newsworthy context or data processed by companies for the purpose of exercising legal and judicial rights would typically and generally be considered legitimate.

Note that matters associated with right of free expression and free speech, breach of privacy and other conducts which may be considered criminal offences

are handled directly by the courts, as the National Data Protection Authority ("*Comissão Nacional de Proteção de Dados*"/CNPD) only handles misdemeanours (criminal activity is reported to the State Prosecutor).

Nevertheless, we note that procedures have taken place before CNPD on this matter. In what specifically concerns the balance between data subject privacy and the search engine's commercial freedom, from May 2014 to May 2017, more than 4.300 Portuguese people officially requested Google remove search results related to their personal data (in practice, hereby exercising their right to be forgotten), with Google´s transparency report stating that 25% of these requests were complied with. As a result, 37 data subjects filed a complaint before CNPD. In this context, CNPD issued 24 decisions. According to the majority of said decisions, Google's refusals were unsubstantiated. Despite the binding nature of CNPD´s decisions, in 4 cases Google chose to proceed to court. The lawsuits are presently pending in the Lisbon Administrative Court.

ROMANIA

Augustin Fuerea

1. Internal Market and electronic commerce : Internet and e-commerce
1.1. Electronic Commerce, liability of Internet intermediaries

Question 1.1.1.

The National Authority for Consumer Protection (hereinafter referred to as NACP) has identified some unsettled issues, which can be considered as difficulties both from the perspective of the market supervisory authorities, as well as of consumers. Difficulties exist in cases where an economic operator, marketing through an online platform (via an intermediary) has its registered office in an EU third country. This country is not subject to EU law, in conclusion, the competent authorities of the Member States cannot intervene, the European consumer being thus deprived of his rights.

Another problem identified by NACP is the liability of the owner of the online platform through which cross-border transactions are made (the intermediary), which has his registered office in a third country and is actively involved in the sale of products and services that can prejudice the European consumers. In such cases, his obligations towards the consumer must be clearly and unequivocally established.

In conclusion, according to NACP, the cross-border online trading with the involvement, in one way or another, of a stakeholder with the headquarters in a third state remains an unresolved issue and consumers involved in such transactions are often, harmed without being able to recover the prejudice and without having the legal remedies against those violations.

In Romania, shows the Competition Council, this form of trade is still going through the early stages of development. The segment is not a mature one, but the rate of growth is accelerating, with the online component playing an increasingly prominent role in defining how companies in the business are developing processes and systems in order to meet consumer demands. These developments are taking place in the context of an increase in internet usage rate of nearly 70%, at national level[1], with maximum values recorded at the level of big urban centres.

Question 1.1.2.

According to Decision no. 1610/2015 of the High Court of Cassation and Justice, Civil Division I, after corroborating provisions of Art. 11 and Art. 14 of the Law no. 365/2002 on electronic commerce, it is clear that the mechanism of liability of the passive internet service provider (which, according to the conceptual meaning described by the CJEU in its Decision ruled in Case L'Oréal SA v. eBay, is the one that does not interfere with the information, having, thus a neutral position with regard to the information provided, since it offers its customers exclusively, technical support by providing a virtual space for the publication of publicly available information] is grafted on the civil liability for another's deed, in the context of the substantive law institutions of national law, and shall be activated only in the cases where the causes of the liability exoneration provided under Art. 14 par. (1) sections a) or b) of Law no. 365/2002 are not incident.

Therefore, the civil liability for damage of the passive service provider, consisting in the permanent storage of the information provided by an addressee of the service, can be involved even when the information is not disseminated by itself but it is only provided on its behalf, meaning by the holders of the sites that have posted the information that directly violates the rights of a third party.

Consequently, in providing publishers of sites whereby sound recordings were reproduced and made available to the public without the consent of the holders of related rights – a virtual space for the permanent storage of this information, whereby, in the absence of authorization by the phonogram producers infringed the rights related to copyright, belonging to them (as provided for by Art. 105, paragraph (1), sections (a) and (g) of Law no. 8/1996 on copyright and related rights, as subsequently amended and supplemented), the passive Internet service provider shall respond according to the provisions of Art. 11 par. (2) of Law no. 365/2002, while its exoneration of liability could only take place if it had been demonstrated that it acted in accordance with the provisions of art. 14 par. (1) section b) of Law no. 365/2002, or whether, having become aware of either the unlawfulness of the information (or activity) or of the potentially

[1] According to data published by the National Institute of Statistics for 2016.

harmful nature of the information, it would have acted quickly in order to eliminate or block access to it.

Question 1.1.3.
No information in the field has been identified.

Question 1.1.4.
No information in the field has been identified.

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.
Examples of problems which NACP has encountered in practice, referring to the remedies contained in the law on guarantees, are:

- removal of the product from the warranty by the service unit (due to improper use) without giving the consumer the opportunity to demonstrate the contract. Furthermore, even if this possibility is given, in most cases the consumer does not have the necessary tools to demonstrate that the product has been properly used;
- returning the product from service with the same effect;
- directing the consumer (by the seller) directly to the service;
- consumers are not provided with both types of guarantees (legal and commercial);
- consumers do not always understand the difference between the legal guarantee and the commercial guarantee;
- vagueness with regard to products falling in the "durable" category.

Question 1.2.2.
According to NACP's point of view, the proposal for a Directive regarding the digital content:

- sets out certain requirements regarding contracts providing digital content, concluded between companies and consumers (business-to-consumer), in particular the rules on the compliance of the digital content with the contract, the remedies available to consumers in the event of non-compliance or non-availability of digital content, as well as aspects regarding the modification and termination of such contracts;
- applies to any contract where the trader provides digital content to the consumer or undertakes to do so, and in exchange, a price is paid or the

consumer actively offers a non-pecuniary consideration in the form of personal data.

Most Member States do not have a legal framework in force in this field, that of marketing the digital content, and there is a legal vacuum also in EU legislation in the field of defective digital content.

Question 1.2.3.
NACP believes that the proposal for a Directive on Digital Content confers new opportunities for both consumers and business, including SMEs, and clarifies a number of issues that are not regulated at EU level, while at the same time contributing to a better functioning of the Single Market by removing barriers created by differences between national legislations in the case of the supply contracts of digital content.

In the opinion of NACP, the proposal for a Directive on the online sale of goods:

- sets out certain requirements for distance contracts concluded between the seller and the consumer, in particular the rules on the conformity of goods, the remedies in the event of non-compliance and the arrangements for the exercise of such remedies;
- does not apply to distance contracts for the provision of services and durable support on which digital content is stored when durable support has been used exclusively as a means of transport for the supply of digital content to the consumer;
- to the extent that they are not covered by this Directive, it does not affect the general provisions on contract law laid down at national level, such as the rules on the conclusion, validity or effects of contracts, including the consequences of the rescission of a contract.

Although consumer protection rules are already harmonized at EU level in some areas, there are still divergences between national consumer contract laws. These divergences generate additional business costs and affect consumer confidence in cross-border shopping, which is why we believe that only full harmonization of the main contractual rights will create a genuine digital single market, beneficial to both consumers and the business community.

Question 1.2.4.
The Commission's legislative initiative of harmonizing the rules on the provision of digital content and the online sale of goods, has the general objective of

diversifying the possibilities offered to both consumers and the business environment by creating a genuine digital single market.

NACP believes that, by removing the main barriers related to contract law which stay in the way of cross-border trade, the rules presented in these proposals will reduce the uncertainty faced by business and consumers due to the complexity of the legal framework as well as the costs borne by the business environment due to differences from the contract law. On the other hand, The Ministry of Communications and Information Society still does not have information on this issue, but intends to centralize in the future the data received from the entities responsible for this.

Question 1.2.5.

Traders[2] who develop online economic activities (through the online contracts for purchase of goods or services providing) have, since January 2016, additional obligations in relation to consumers who benefit from their services or products. In case of non-compliance, the fines reach up to 5,000 lei. Starting from January 9, the provisions of Regulation no. 524/2013 on online dispute resolution in the consummation field are applied. These provisions oblige all traders in the European Union who conclude online sales or service contracts to provide an electronic link to the online dispute resolution (ODR) platform on their websites. The ODR platform is designed as an online tool developed by the European Commission and acts as a single point of entry for consumers and traders seeking out-of-court settlement of disputes arising from online transactions. The link must be easily accessible to consumers and retailers. They also need to specify their email addresses. The failure to comply with this obligation is sanctioned by the National Authority for Consumer Protection (NACP) with a fine between 2,000 and 5,000 lei. At present, Romanian traders may, technically comply with this legal obligation and, therefore, strictly with respect to this obligation, may be fined if they do not provide the electronic link to the ODR platform on their web pages.

In addition to the above obligation, which is addressed to all economic agents, there is an additional obligation. This is only applicable to those traders who have engaged or are required to use one or more ADR entities (alternative dispute resolution) to resolve disputes with consumers. Thus, these traders must inform consumers about the existence of the ODR platform, but also about the possibility for consumers to use this platform to resolve their disputes. In this regard,

[2] The information for this response has been downloaded from the https://www.avocatnet.com/articol_42666/Firmele-cu-magazine-online-au-noi-obliga%C8%9Bii-a-c%C4%83ror-nerespectare-se-poate-sanc%C8%9Biona-cu-pan%C4%83-la-5000-de-lei.html

those traders provide an electronic link to the ODR platform on their website and, if the offer is submitted by e-mail, in that e-mail. Again, the non-compliance with the above is punishable by NACP with a fine between 2,000 and 5,000 lei.

Question 1.2.6.
No information in the field has been identified.

Question 1.2.7.
The Ministry of Communications and Information Society through the strategies and policies envisaged for the next period will consider these issues.

Question 1.3.1.
The Ministry of Communications and Information Society considers it appropriate to improve cooperation between Member States in order to improve the conditions offered by traders, as well as strengthening consumer protection mechanisms and eliminating any possible elements of discrimination.

1.4. Questions related to the collaborative economy

Question 1.4.1.
As it results from the point of view of the Ministry for the Business, Trade and Entrepreneurship Environment, the Single Market Strategy presented by the European Commission on 28 October 2015 (COM Communication "Single Market Improvement: More Opportunities for Citizens and Enterprises") proposes a series of practical measures designed to create new opportunities for consumers, professionals and businesses, support the development and expansion of small and medium-sized enterprises (SMEs) and start-ups, promote innovation and stimulate investment.

A priority objective of the Single Market Strategy is to stimulate the cross-border provision of services, the measures to this end aiming at removing barriers still present in the Single Market at more than 10 years after the adoption of the European Parliament and Council Directive 2006/123/EC on services in the Internal Market (the Services Directive).

In the national legislation, the Services Directive has been transposed, horizontally, by Government Emergency Ordinance (GEO) no. 49/2009 on the freedom of establishment of service providers and the freedom to provide services in Romania, approved with amendments and completions by Law no. 68/2010.

The implementation of provisions of the Services Directive, transposed by Government Emergency Ordinance no. 49/2009, is carried out in several sectors of activity, involving several responsible institutions, with attributions in the field of both the central administration and the local administration.

However, according to the point of view of the Ministry of Business, Commerce and Entrepreneurship, no authority of the Romanian state has so far coordinated the implementation of this directive at national level.

Thus, cross-border administrative cooperation between national authorities in the area of the internal market, including the Services Directive, is therefore achieved through the Single Market Information System (IMI). The responsibilities of IMI National Coordinator for Romania are fulfilled by the Legislative Harmonization Directorate (DAL) within the Ministry of Foreign Affairs, which also fulfils the role of coordinator of legislative area, alert reception centre and service notifying coordinator.

The single point of contact (SPC) provided by the Services Directive to operate in all Member States as a one-stop-shop for service providers, both for obtaining information and for performing administrative procedures through electronic procedures, is ensured, in Romania by the Agency for the Digital Agenda of Romania.

Question 1.4.2.

According to the Competition Council, the entry of new competitors on the market often produces beneficial effects for consumers, through several aspects: new services, innovations or lower prices. This effect has been seen in recent years when the entry of new competitors into traditional markets has materialized in new services, often more innovative, more accessible and more suited to current consumer demands.

The Competition Council considers that the technological advance facilitated the market entry of atypical economic actors, which rival successfully with the ones on the traditional markets. The most relevant examples in this regard are cases on the passenger transport market (Uber vs. Taxi) or on the accommodation market (Airbnb/HomeAway vs. hotel accommodation services). Moreover, new services have the capacity to generate macroeconomic effects: reducing transaction costs and informational asymmetries (search and information costs are often low), as well as the more efficient use of available capital in an economy.

Question 1.4.3.

The Agency for the Digital Agenda of Romania (hereinafter referred to as ADAR) has an important role to play in this area, of requirements imposed on providers for access to obtaining authorizations. It is important to emphasize the importance of ADAR to the development of the digital economy from the perspective of managing the electronic systems that the institution operates.

From the perspective of generally valid principles of the digital economy development, namely accessibility and availability, ADAR, a public institution of

the central public administration, supports consumer needs by providing easy-to-use computer systems that meet their needs through obtaining benefits electronically without the applicant going to the physical point of the service provider.

ADAR contributes to the development of the digital economy by:

- Creating new interactions between citizens and the central and local public administration authorities;
- Freedom of access to information for consumers;
- Transparency of actions resulting from the citizen's interaction with central and local public administration;
- Implementing national legislation transposing EU legal acts on accessibility of services;

Among the systems managed by ADAR and contributing to the development of the digital economy are: The Electronic Public Procurement System (EPPS)[3]; the Single Electronic Contact Point (SECP)[4] and the National Electronic Payment System for Fees and Taxes using the Banking Card (NEPS)[5].

Through the Single Electronic Contact Point (SECP) users, both in the country and in the EU can obtain some authorizations/approvals by initiating and completing the request entirely electronically.

Authorization procedures are configured in SECP by central and local government institutions, some of which are streamlined and standardized to facilitate user access to obtaining a service/benefit.

Running a procedural flow to obtain authorizations/approvals is transparent, the applicant knowing at any time the status of the dossier under analysis at the public institution.

The Ministry of Communications and Information Society has not registered with the providers any difficulties related to the approval and authorization process.

[3] The public utility information system, accessible via the Internet at www.e-licitatie.ro, used for the purpose of public procurement by electronic means. The use and functioning of EPPS is carried out in accordance with the legal provisions on public procurement, through electronic auctions. The legislation governing public procurement is available at: https://www.aadr.ro/legislatie_0_13.html

[4] The Single Electronic Contact Point (SECP) accessible at www.edirect.e-guvernare.ro is an IT system of public utility, an integral part of the e-government system through which permits/authorizations/certifications/qualifications are obtain electronically. For the legislation governing SECP, see: https://www.aadr.ro/legislatie_0_13.html

[5] Accessible at www.ghiseul.ro, NEPS is a component part of the national electronic system and allows online card payment of local taxes and fees as well as car fines. To view the legislation that implements Ghiseul.ro, please visit: https://www.aadr.ro/legislatie_0_13.html

Question 1.4.4.
According to NACP, the main consumer issues that have arisen on the EU market with the rapid development of this type of collaborative economy can pose challenges for both market supervisory authorities and consumers. Collaborative economy refers to business models where activities are facilitated by collaborative platforms that create an open market for the temporary use of goods or services often provided by individuals. One of the biggest legal challenges is that EU legislation in the field of consumer protection in many Member States does not apply to transactions between individuals and in this case, there is a problem when irregularities occur with the products or services marketed.

Question 1.4.5.
NACP points out that a problem that is currently being discussed at Member State level is that of the conditions under which, in the context of a sale of goods or services from individual to individual, natural persons, the one who sells qualifies himself as a trader. Member States are currently approaching this issue differently. At EU level, this issue is assessed on a case-by-case basis. In this respect, the Commission gives some general guidance in the revised Guidelines on the Directive on Incorrect Trade Practices, but it is not sufficient as the cases that may arise are very diverse.

Question 1.4.6.
At present, NACP reports that there are no clear obligations and rights stipulated by law for the factors involved in the collaborative economy. The issue is somehow regulated at national level in 14 EU Member States, but there is a need for EU-wide measures to have harmonized, unitary and clear regulations that apply in the collaborative economy for all types of sales.

With regard to how to increase consumer confidence in peer-to-peer services, NACP believes that online ratings/reviews of other consumers who have benefited from these services and trusted labels can be appropriate tools to fill the lack of information on the supplier service, natural person.

However, online ratings/reviews are limited ways and there is no certainty that they are real or not, so they can not be a guarantee that the services provided by that individual comply with what it is described on the online platform through which the transaction takes place. The uniform EU legislation could be a solution to develop this type of economy and to increase the level of the consumer's confidence in the collaborative economy. On the other hand, The Ministry of Communications and Information Society believes that these mechanisms contribute to increasing consumer confidence in this type of service.

2. Digital media

Question 2.1.

The definition of the audiovisual media service, as set out in the current Audiovisual Media Services Directive, hereafter referred to as AVMSD) covers only television services and on-demand services, the latter being mainly present on the Internet.

The reasoning 28 of AVMSD states that the scope of this directive should not include electronic versions of newspapers and magazines, this reasoning being introduced at the request of media organizations.

AVMSD does not apply to the content provided by intermediaries/distributors via online platforms. These platforms and these intermediaries are mainly regulated by the E-commerce Directive, which releases them from liability for the content they transmit, store or host.

Romania has transposed the requirements of Directive 2010/13/EU into national legislation through the Audiovisual Law no.504/2002, as subsequently amended and supplemented, NAC Decision no.220/2011 on the Audiovisual Content Regulatory Code, as subsequently amended and supplemented, and, respectively, NAC Decision no.320/2012 on the provision of on-demand audiovisual media services.

With regard to the CJUE judgment (C-347/14), such a preliminary ruling under Article 267 TFEU is binding and the interpretation given makes it a common body with the interpreted act. Consequently, the Decision of the Court of Justice of the European Union could not lead to a different approach in Romania. The National Audiovisual Council (hereinafter referred to as NAC) has no relevant practice in this matter, since it has not analyzed and issued no sanctioning decision for such a case.

The NAC notes that in the debates on amending and supplementing this directive, the interpretation given by the CJEU to the notion of "programme" in Directive 2010/13/EU has provided legal arguments for extending the current scope. According to the CJEU, a video section which on a website qualifies as an on-demand audiovisual media service does not lose this feature simply because it is accessible on the website of a newspaper or because it is proposed within it. Such video recordings compete with programmes offered by television services. According to the CJUE, the assessment of the main purpose of a service of providing video recordings offered in the electronic version of a newspaper should be made by examining whether that service, as such, has content and an autonomous function in relation to those of the journalistic activity of the operator of the website in question, and are not just an indispensable complement to this activity, in particular because of the links that the audiovisual offer presents with the textual offer. The task of this assessment goes to the regulatory authority, or, as the case may be, to the court.

Question 2.2.

The Ministry of Communications and Information Society, through its quality, permanently contributes to the improvement of the legislative/normative framework so as to ensure effective protection of minors against online content, even if these aspects are already foreseen in the current legislation.

According to the NAC, based on CJUE Decision (C-347/14), the introduction of video platforms (such as YouTube) into the scope of the AVMSD could not be avoided.

NAC considers it positively to impose equivalent regulatory conditions for the content offered by Internet platforms to ensure that they take appropriate measures for each type of platform in order to protect minors from harmful content, and the public, in a broad sense, to be protected from incitement to hatred.

The NAC notes that, in the debate on the proposal to amend the AMSVD, the scope extends beyond what it was proposed in the original text, and social media services are also included in the scope of the directive. The NAC believes that the reasoning for expanding the scope of the AVMSD by including social media services can be justified, but putting it into practice with technical means of monitoring and control specific to classical television services will be a challenge for authorities, hard to quantify at this time. For example, it will be difficult to separate the content intended for the general public from the one addressed to a small group of users (e.g. Facebook), or it will be difficult to find a violation in the case of a live streaming video content that can be claimed after its deletion on the website. From our point of view, in the case of live streaming, the most effective way at the moment would be a Code of Good Practice adopted by industry (e.g. Facebook) under the coordination of European institutions.

Regarding the level of harmonization of online sharing platforms, the Member States' views are divergent. Some Member States aim at maximizing the harmonization of online platforms, while other states are supporting the minimum protection – where competencies are left to Member States through the co-regulation mechanism, a variant that the Romanian regulation authority has also supported.

With regard to commercial communications on video sharing platforms, the NAC considers that they are already covered by Directive 2005/29/EC on unfair business-to-consumer commercial practices on the internal market, which prohibits unfair business practices of companies towards consumers, including deceptive and aggressive practices occurring within the information society services. As regards to the commercial communications on tobacco products from video sharing platforms, the existing prohibitions laid down in Directive 2003/33/EC on the harmonization of laws, regulations and administrative provisions of the Member States relating to video- advertising and sponsorship in

favour of tobacco products are applicable, as well as the prohibitions applicable to communications on electronic cigarettes and refill bottles under Directive 2014/40/EU on the approximation of laws, regulations and administrative provisions of the Member States relating to the manufacturing, presentation and sale of tobacco products and related products, regulations providing sufficient consumer protection.

Preamble 27 of the AVMSD specifies the nature of the legal relationship between the provisions laid down in the sectoral directives – Directives 2005/29/EC, 2003/33/EC and 2014/40/EU and, on the other hand, AVMSD provisions, in the sense that measures provided in AVMSD complement those measures set out in the three sectoral directives. From this perspective, it will be necessary to coordinate the legislative transposition of these directives, especially regarding the sharing of competences between the responsible national authorities (in the case of Romania, CNA, ANPC, The Competition Council and The Ministry of Public Finance). This coordination will be all the more necessary as rules extend to sharing platforms.

Question 2.3.

The proposed amendments to the AVMSD review project aim at strengthening the application of the principle of the country of origin that underpins the free movement of services in the EU.

Among the amendments introduced in the AVMSD review draft, NAC also notes the obligation for Member States to establish and communicate to the Commission, the list of audiovisual media service providers, specifying the jurisdictional criteria applied in each individual case. In the opinion of NAC, the list of audiovisual media service providers under the jurisdiction of a Member State should be supplemented by additional information, such as the targeted audience (the destination countries of the service) and the language versions of the programmes. At the same time, the NAC also noted that the establishment of jurisdiction on the basis of the daily frequency of the editorial decision provided in the initial text would be likely to create legal uncertainty. According to NAC, it would be necessary to introduce the requirement of continuity in editorial decisions, including in cases where, by the technical and editorial nature of the platform, it is exercised with a certain periodicity.

National audiovisual markets with a low penetration potential in other audiovisual markets will always have the tendency, which can be argued, to question the country of origin principle. And in Romania, such trends, expressed by Romanian broadcasters, faced with an increasing competition, have been manifested in time.

The NAC affirmed the need to respect the principle of freedom of reception and retransmission, as well as that of the country of origin, on which the

Audiovisual Media Services Directive 2010/13/EU is based. Based on the jurisdiction criteria set out in the Audiovisual Media Services Directive (AVMSD), only Romanian television stations under Romanian jurisdiction are subject to Romanian legislation. The European Commission, supported by the decisions and jurisprudence of the EU Court of Justice, did not accept any compromise that would allow any form of exercise of double control, even secondary, to the same television station. Therefore, no State can limit (for reasons related to the fields coordinated by the Directive) the reception and/or retransmission on the national territory of programmes broadcasted by broadcasters under the jurisdiction of another State.

According to Article 75, paragraph (2) of the Audiovisual Law "the retransmission on the Romanian territory of programme services broadcasted by broadcasters under the jurisdiction of the Member States of the European Union is free and does not require any prior authorization". According to the provisions of paragraph (3) of the same Article, the Council can temporarily restrict the right to free retransmission of a particular service of programmes from the Member States of the European Union if the following conditions are cumulatively fulfilled:

a) the service of programmes violates explicitly, significantly and seriously the provisions of art. 39 or 40; (...).

The provisions of art. 75 of the Audiovisual Law transpose the provisions of art. 3 and 4 of AVMSD. In accordance with the provisions of art. 3 par. (1) of the AVMSD, Member States must ensure the freedom of reception. The MS cannot restrict the retransmission on their territory of audiovisual media services under the jurisdiction of other MS, for reasons falling within the fields coordinated by this Directive. Article 3, paragraph (2) of the AVMSD provides an exception to this general rule, if a television transmission from another MS seriously and gravely violates the provisions of art. 27 par. (1) or par. (2) and/or art. 6 of the AVMSD. These articles refer to the protection of minors, respectively, to the incitement to hatred.

In a series of decisions, the EU Court of Justice clarified the fundamental provisions of the Audiovisual Media Services Directive on concepts of national competence, jurisdiction, freedom of reception and retransmission, laying down the following principles:

1. Each State is responsible to the community, for the effective enforcement of its own legislation by broadcasters under their jurisdiction;
2. No State may, for reasons connected with the fields coordinated by the Directive, limit the reception and/or retransmission on the national territory of programmes broadcasted by broadcasters under the jurisdiction of another State.

Based on the jurisdictional criteria set out in the Audiovisual Media Services Directive, only television stations under Romanian legislation are subject to Romanian jurisdiction. The inclusion in the service of programmes of some commercial communications addressed to the public in the Member States in which it is retransmitted or the language version do not constitute criteria provided in the AVMSD.

According to art. 75 par. (2) of the Audiovisual Law "the retransmission on the Romanian territory of the services of programmes broadcasted by broadcasters under the jurisdiction of Member States of the European Union is free and does not require any prior authorization".

The NCA further states that there have been no disputes in our country regarding the application of the principle of the country of origin and there have been no significant legal problems with providers established outside the EU and targeting the public in our country.

Question 2.4.

NAC supported, along with other Member States, the introduction of administrative, financial obligations for Member States to support the independence and effectiveness of regulatory authorities. The principle of independence of the national regulatory authorities in the audiovisual field is a reference point in the EU space, each Member State having competent and specially appointed authorities in the audiovisual field, a complex and rapidly evolving sector. Moreover, this principle is extended and protected at the level of all Member States of the Council of Europe, being directly attached to the universal system of values protected by the European Convention on Human Rights.

Under the provisions of the Audiovisual Law no. 504/2002, as amended and supplemented, the National Audiovisual Council is "an autonomous public authority under parliamentary control and guarantor of the public interest in the field of audiovisual communication". The Council is a unique regulatory authority in the field of audiovisual media services, under the conditions and in compliance with the provisions of the law, and as a guarantor of the public interest in the field of audiovisual communication. The Council has a set of obligations and duties.

The Ministry of Communications and Information Society did not notice any dysfunctionality in relation to these issues, ascertaining that a balanced competitive environment is established at national level.

2.5.

As regards to the implementation of the audiovisual legislation, in practice, situations that required intervention by the regulator are inevitable, and they also

have the role of providing unitary interpretations through the tools offered by the law (recommendations, instructions, summons or, as a last resort, sanctions). Such interventions, in the specific cases, were in most cases regulated (protection of minors, commercial communications, protection of the human dignity, etc.).

Regarding the legal provisions in force, those concerning the must-carry obligations provided in Art. 82 of the Audiovisual Law no. 504/2002 were subject to exceptions of unconstitutionality, rejected by the Constitutional Court (Decision No. 266/2013 and Decision No. 426/2012). However, in the opinion of the NAC, it is necessary to adapt the rules on the must-carry regime to the purpose for which they were set up, taking into account the current developments of retransmission platforms; the reasons for imposing such obligations are: ensuring broad accessibility, especially for local or regional posts, and the need to guarantee the public, a pluralistic programme offer.

The Ministry of Communications and Information Society noted that these issues are properly regulated and monitored by the National Audiovisual Council.

Question 2.6.
Within the two major categories of currently regulated audiovisual services (television services and on-demand media services), the NAC did not see the use of such techniques to direct advertising or personalized content.

The NAC appreciates that regulatory authorities should be prepared to cope with such new issues as the expected adoption of the AVMSD, such as the use by intermediaries, of such online targeting techniques.

Question 2.7.
No information in the field has been identified.

Question 2.8.
The Ministry of Communications and Information Society aims to analyze these issues in the next period.

3. Digital infrastructures

Question 3.1.
According to the National Authority for Administration and Regulation in Communications (hereinafter referred to as ANCOM), before the adoption of Regulation (EU) 2015/2120, in Romania there was no legal framework allowing or prohibiting traffic management or other practices related to net neutrality. However, the legal framework imposed on the providers of electronic communication services transparency obligations related to traffic management practices, as a transposition of the provisions of articles 20 and 21 from the Universal Service

Directive (Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services). This legal framework is still in force and complements the provisions of Regulation (EU) 2015/2120.

Regarding zero-rating cases, ANCOM does a case-by-case assessment, according to the BEREC Guidelines, of the zero-rating practices which are not explicitly prohibited by the Regulation. ANCOM has requested official information about zero-rating practices from all mobile operators in Romania and an in-depth analysis will be carried out with regards to all the offers containing such practices that could represent a problem from the point of view of the 2015/2120 Regulation.

The Ministry of Communications and Information Society did not find any problems on the subject of neutrality.

Question 3.2.

ANCOM mentions The current regulatory framework fostered the setting of several alternative providers, allowed the entering into national market of providers from various Member States and provided an important level of protection for the consumers' rights. We underline that this outcome was reached despite factors which worked against. For instance, we believe that the taxation rules applicable to cross border electronic communications services until the end of 2014 worked strongly against the development of internal market. Distinct VAT rates depending upon the customer, whether consumer or business is, did not actually promote the provision of cross-EU electronic communications services.

According to ANCOM, as regarding general authorization, for certain providers of European relevance it would be simpler to pass a notification procedure to a European body than to the national public authorities of each Member State in whose territory they intend to provide electronic communications networks and services. On the other hand, most of the suppliers are of national relevance and the passing of the notification procedure to a European body would only make it more difficult to meet this requirement (e.g., barriers of a linguistic nature). In these circumstances, we feel that a single European notification format could be agreed and a standard set of documents to be attached to the notification form and providers should be given the freedom to choose between completing the notification procedure before a European body or before a national public authority, as would be easier for them.

Another subject for possible EU level harmonization could be the tariffs for call termination that are significant different between members states, despite the existence of Recommendation 2009/396/CE on the Regulatory Treatment of Fixed and Mobile Termination Rates in the EU.

According to ANCOM, the Romanian authorities have adopted different measures dedicated to stimulating the development of broadband networks, most of them being the result of initiatives at European level. For example, a National NGN Infrastructure Development Plan has been adopted, various state aid projects have been initiated to develop broadband infrastructure in uncovered areas, etc.

The Ministry of Communications and Information Society initiated a large-scale development of NGN-wide networks of its own initiative with European funding.

Question 3.3.
These issues are properly regulated and monitored by ANCOM.

Question 3.4.
The Ministry of Communications and Information Society is not aware of the existence of such problems.

4. Data in the digital economy

Question 4.1.
Regarding the measures for the application of Regulation (EU) 2016/679, the National Supervisory Authority for Personal Data Processing (hereinafter referred to as the Supervisory Authority) states that since the Ministry of Internal Affairs has conducted negotiations at the Committee meeting for Data Protection and Information Exchange – DAPIX from the EU Council on the personal data protection package, it initiated the Memorandum on the Transposition into National Legislation of the European Parliament and Council Directive (EU) 2016/680 of 27 April 2016/679 of the European Parliament, as well as of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and on repealing Directive 95/46/EC .

Through this Memorandum, the Inter-Ministerial Working Group was set up in order to ensure that measures were taken regarding the direct application of the provisions of Regulation (EU) 2016/679 and the transposition of Directive (EU) 2016/680, coordinated by the Ministry of Internal Affairs.

In the context of discussions within the Group, the Supervisory Authority participated actively in the preparation of the draft Law for amending and completing the Law no. 102/2005 on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing, as well as for repealing the Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

as well as the Explanatory Memorandum. This draft law aims at implementing some provisions of the Regulation, namely the provisions of art. 51-55, 57-59, 62, 77, 79, 80, 82-84.

Therefore, at present, the above-mentioned draft law is in the approval procedures provided in the Government Procedures Regulation for the elaboration, endorsement and presentation of draft public policy documents, draft legislative acts, as well as other documents, for adoption/approval, adopted by Government Decision no. 561/2009. This project is to be presented to the Romanian Parliament in September. Also, according to the Supervisory Authority, within the Inter-Ministerial Working Group, the draft Law on some measures for implementing the Regulation (EU) 2016/679 is also under consideration.

The Ministry of Communications and Information Society is involved in the process of legislative harmonization in this direction, the proposals being in the process of finalizing the approval process.

Question 4.2.

Since 2016 until now, the Supervisory Authority has participated in data protection events organized by private entities. During these meetings, the representatives of the institution presented the novelty of the General Regulation on Data Protection, as well as aspects related to the legal conditions of data usage, the respect of the rights of the data subjects and the confidentiality of the personal data processing.

In this respect, we mention that presentations were held at roundtables, conferences, seminars, etc., organized by various professional associations from different fields of activity, which brought together a considerable number of participants.

The Supervisory Authority notes that, in order to ensure the uniform application, from 25 May 2018, of Regulation (EU) 2016/679 – the General Regulation on Data Protection, the Article 29 Working Group adopted and published a series of guides. These guides, in English, as well as their non-official translation into Romanian by the Supervisory Authority, as well as other documents, are available on the Supervisory Authority's website, www.dataprotection.ro, in the section dedicated to the New General Regulation of Data Protection, http://www.dataprotection.ro/?page=Regulamentul_nr_679_2016, also available in English. At the same time, the above section also contains information on various actions carried out by the Supervisory Authority or events attended by its representatives, to popularize the New General Regulation on Data Protection. The Ministry of Communications and Information Society did not notice any malfunctions in this direction.

Question 4.3.
With regard to the areas listed, the Supervisory Authority stresses the need to respect the legal framework in the field of data protection and the requirements of the new European Regulation on Data Protection (*Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the protection of individuals on the processing of personal data and on the free movement of such data*, which will be directly applicable starting from 25 May 2018).

At the same time, the Supervisory Authority states that on 10 January 2017, the European Commission published the proposal for a Regulation on privacy and protection of personal data in electronic communications and for repealing Directive 2002/58/EC (the Regulation on private life and electronic communications – ePrivacy). On this issue, the Ministry of Communications and Information Society has been designated as the coordinating and responsible ministry for establishing Romania's mandate for external meetings on the ePrivacy Regulation, with the support of the other institutions involved in the negotiation process of the legislative package on data protection, respectively the Ministry of Internal Affairs, the Ministry of Justice and the Ministry of Foreign Affairs, the National Supervisory Authority for Personal Data Processing, the National Authority for Administration and Regulation in Communications, the National Centre of Response to Cyber Security Incidents.

By doing so, the Supervisory Authority shows that Working Group 29 has issued, in connection with the *Internet of Things* concept, Opinion 8/2014 on recent developments in the Internet of Things field that can be consulted by accessing the link: http://ec. europa.eu/justice/data-protection/article-29/documentation/opinion- recommendation/files/2014/wp223_en.pdf

The Ministry of Communications and Information Society did not notice any malfunctions in this direction.

Question 4.4.
On this point, the Supervisory Authority notes that, from May 2014 (after the CJEU decision) and until now, the Authority has received over 100 petitions aimed at deleting the results displayed on the Internet using Google's search browser, having their name and surname as criterion.

The Supervisory Authority has reviewed each complaint if it is admissible and if there are sufficient relevant elements for the soundness of the requests received. In performing this analysis, the criteria set out in the judgment of the Court of Justice of the European Union in the Costeja case of 13 May 2014 and the "Guide to the application of the judgment of the Court of Justice of the European Union on" Google Spain and INC V. Agencia Español de Proteccion

de Datos (EDPS) Mario Costeja Gonzales "C-131/12", adopted on November 26, 2014 by the Art. 29 Working Group, which includes the Romanian supervisory authority have been considered.

If a complaint is considered admissible and well founded, the Supervisory Authority initiates an investigation requesting Google Inc. to respond to the request.

To this end, the Supervisory Authority states that complaint models, as well as the Procedure for receiving and solving complaints, notices and applications, are available at http://www.dataprotection.ro/?page=cerere&lang=en. Furthermore, regarding the ability of a targeted person to submit a request for deletion of data to Google, one can find on the institution's site the address that can be used by individuals in such situations, namely https://support.google. com/legal/contact/lr_eudpa? product = websearch & hl = en.

In this context, the Supervisory Authority mentions that there have been 3 cases where the addresses issued by the Authority in order to resolve the requests received for deletion of personal data from the search browser were appealed in court. For two of these, the court ruled in favour of the Supervisory Authority, while the third case is still pending.

SLOVENIA

Matija Damjan*
Klemen Podobnik**
Ana Vlahek***

1. Internal Market and electronic commerce: Internet and e-commerce

1.1. Electronic Commerce, liability of Internet intermediaries

The regime of liability of Internet intermediaries as set out in the E-Commerce Directive is transposed into Slovenian law in Chapter 2 of the Electronic Commerce Market Act (ECMA).[1] In line with the directive, ECMA distinguishes between three types of intermediary services: mere conduit, caching and hosting. The main principle is that service providers are under no general obligation to monitor the information which they transmit or store, nor actively to seek facts or circumstances indicating illegal activity. Under the notice-and-takedown system, they must act only when they are aware of the illegal content hosted or when the injured party informs them about the violation. ECMA reproduces, more or less literally, the provisions of the directive, but provides little additional guidance on issues not clarified by the directive. For example, the law does not specify the circumstances in which intermediary service providers should be considered aware of an unlawful activity or information. Slovenian courts have held that a hosting service provider was obliged to take down the illegal content only after having been notified of the specific violation by the affected party.[2] Similarly,

* Assistant Professor, PhD, Institute for Comparative Law at Faculty of Law in Ljubljana.
** Associate Professor, PhD, University of Ljubljana, Faculty of Law.
*** Associate Professor, PhD, University of Ljubljana, Faculty of Law.

[1] Sl. *Zakon o elektronskem poslovanju na trgu (ZEPT)*, Official Gazette of RS, No. 61/06, with further amendments.

[2] Judgement of the High Court in Ljubljana, ECLI:SI:VSLJ:2012:I.CP.3037.2011; order of the same court, ECLI:SI:VSLJ:2013:I.CPG.862.2013.

the administrator of an online forum was not obliged to check the truth of all posts, but had to react to the received notification and remove any offensive and illegal messages.[3] However, after the notification, the service provider must take action immediately and not wait until the unlawfulness has been established by a court order or a judgment.[4]

Article 11 of the ECMA provides that service provider is exempt from liability if they act immediately after obtaining knowledge of unlawfulness to remove or to disable access to the illegal content. The law does not define the standard of immediacy, so it is not clear whether the service provider must act instantly after receiving a takedown notice or whether they can take appropriate time to check the facts and obtain legal opinion in cases where illegality of content is not evident at first sight. The law also does not specify the form of a takedown notice which obliges a service provider to act. Thus, it remains unclear whether the request must be in writing or whether a telephone call or an SMS message suffices. Furthermore, it is unclear whether the request can be anonymous or whether the sender should identify themselves as the rightsholder and specify the rights that the contested content allegedly infringes. The existing case law under the ECMA has not yet addressed these issues.[5]

Concerning legal grounds for intermediate service provider's liability, the High Court in Ljubljana held that disregarding a takedown request does not make the service provider automatically liable for the disputed content, but merely rescinds their immunity from any claims, whereas the merit of such claims must still be assessed under the general rules of civil or criminal law.[6] No cases are reported where Slovenian courts would apply the test of technically neutral service provider, devised by the CJEU in *Google France v. Louis Vuitton (AdWords)* and *L'Oréal v. eBay*. However, the existing national case law does not in any way contradict this test.

The ECMA provides in Articles 9 to 11 that a court may order the service provider to stop or prevent an infringement. The court may order the removal of or disabling access to illegal content for the purpose of detecting and preventing criminal offenses, protection of privacy, protection of classified information or business secrecy. Article 18 further provides that anyone who believes that the service provider is in breach of their rights may request the competent court to issue an injunction ordering the service provider to remove or disable access to the infringing information. The courts have held that this allows issuing an

[3] Judgement of the High Court in Ljubljana, ECLI:SI:VSLJ:2017:I.CP.3097.2016.

[4] Judgement of the High Court in Ljubljana, ECLI:SI:VSLJ:2014:I.CP.252.2014.

[5] See M. Damjan, *Odgovornost ponudnikov storitev informacijske družbe in spletnih medijev za uporabniške vsebine*, Pravosodni bilten, 2017, vol. 38, no. 1, pp. 153-177.

[6] Judgement of the High Court in Ljubljana, ECLI:SI:VSLJ:2017:I.CP.289.2017.

injunction to order the removal of a blog post violating a person's reputation and good name.[7] No injunctions for advance filtering of the content, such as in *Scarlet v SABAM*, have been filed for before Slovenian courts.

A not yet clearly resolved issue in the national case law remains the relationship between the provisions of ECMA and of the Media Act[8] concerning the liability of online media. The High Court in Ljubljana held in 2013 that an online forum may correspond to the definition of mass media, reasoning that the forum rules were comparable to an editorial policy and the limitation of the discussion on a particular subject meant that the purpose of the forum was to transmit information to the general public.[9] Nevertheless, the court only applied the provisions of ECMA when deciding on an injunction to remove the disputed posts. In other similar cases, the courts have held that provisions of ECMA are to be applied regardless of whether the defendant is considered a media publisher or not.[10]

An amendment to the Media Act adopted in March 2016 inserted a new paragraph into Article 9, which requires all media publishers who allow the public to post comments on their website to adopt commenting rules and to take down any comment that does not comply with these rules as soon as possible and no later than one working day after receiving a report of the inappropriate comment. Interestingly, the law in no way defines the content of the commenting rules, but leaves it entirely to each media publisher's self-regulation. Since provisions of the Media Act have to be applied in conjunction with the ECMA, it remains to be seen if and how these new rules affect the liability of online media for readers' comments. Can a media publisher who did not act as a technically neutral intermediary in the sense of *L'Oréal v. eBay*, but encouraged their readers to post objectively offending comments, still be found immune from liability as long as such comments are removed upon affected party's request? In any case, Media Act provisions only apply to intermediary service providers with the status of mass media, which are entered in the media register at the Ministry of Culture. The obligation to adopt commenting rules does not apply to social networks and blogs, even if the comments in them can refer to articles published in online media.

[7] Order of the High Court in Koper, ECLI:SI:VSKP:2017:CPG.15.2017.

[8] Sl. *Zakon o medijih (ZMed)*, Official Gazette of RS, No. 35/01, with further amendments.

[9] Order of the High Court in Ljubljana, ECLI:SI:VSLJ:2013:I.CPG.862.2013.

[10] Judgement and order of the High Court in Ljubljana, ECLI:SI:VSLJ:2014:I.CP.252.2014; judgement of the High Court in Maribor, ECLI:SI:VSMB:2015:I.CP.11.2015.

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.

Directive 1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees (hereinafter: Directive 1999/44)[11] was implemented into Slovenian legal system in January 2008[12] by the amendments made to the Consumer Protection Act of 1998 (Sl. *Zakon o varstvu potrošnikov (ZVPot)*, hereinafter: CPA) being the focal piece of legislation in the field of consumer protection.[13] The Directive was implemented in Chapter VI of the CPA (Articles 37-37.č CPA).[14] With regard to questions that are not covered in the CPA, the Code of Obligations of 2001 (hereinafter: CO)[15] applies. If the object of a sales contract is an apartment or a single occupancy building, specific provisions of the Act on Protection of Buyers of Apartments and Single Occupancy Buildings apply in specific types of relationships and specific factual circumstances.[16] The remedies' regime under this act is similar, but not identical to that in the CPA.[17]

[11] Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees, OJ L 171, 7.7.1999, pp. 12-16. Amended by Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (Text with EEA relevance), OJ L 304, 22.11.2011, pp. 64-88.

[12] Act Amending the Consumer Protection Act, Official Gazette of RS, No. 126/07. The new provisions entered into force on 15 January 2008.

[13] So far, the CPA has been amended seven times in 2002, 2004, 2007, 2009 and in 2011. The majority of the amendments have implemented the EU consumers' directives. The most extensive amendment was made in 2002 before Slovenia had joined the EU in 2004. The Slovenian Constitutional Court has also assessed constitutionality of one of the CPA's provisions in 2006 regarding the duty to communicate with the consumers also in Italian and Hungarian language in the territories of Italian and Hungarian minorities (Decision of the Constitutional Court of RS, no. U-I-218/04-8 of 20 April 2006, Official Gazette RS, no. 46/2006). For further details on the evolution of Slovenian consumer protection legislation, see A. Vlahek, *Consumer Protection in Slovenia*, in: H. Barancová, P. Blaho, J. Lazar (Eds.), Rechtsschutz des schwächeren Subjekts im Privatrecht : XI. Dies Luby Iurisprudentiae, Spectrum Slovakia series, vol. 6, Frankfurt am Main, Peter Lang; Trnava, University of Trnava. 2014, pp. 129-146.

[14] The CPA consist of the following chapters: I General provisions; II Liability for dangerous products; III Advertising of goods and services; IV Warranty; V Contractual terms; VI Sale of goods and performance of services (1. General rules; 2. Rules on the characteristics of goods; 3. Pre-payment; 4. Specific types of contracts (a. Delivery of goods to the consumers; b. Distance selling; c. Doorstep selling; d. Distance financial services); 5. Instalment sale; 6. Package travel; 7. Time-share); VII Agencies for the protection of consumers; VIII National Programme of consumer protection; IX Inspection control and administrative measures; X Private enforcement; XI Provisions on misdemeanour; XII Final provisions.

[15] Sl. *Obligacijski zakonik (OZ)*, Official Gazette of RS, No. 83/2001, with further amendments. The CO entered into force on 1 January 2002.

[16] Sl. *Zakon o varstvu kupcev stanovanja in enostanovanjskih stavb (ZVKSES)*, Official Gazette of RS, No. 18/04.

There are quite some inconsistencies and ambiguities in the CPA that has unfortunately not been drafted very thoroughly and lacks precision and perfection.[18] As will be shown below, Directive 1999/44, too, has not been implemented with much consideration. Although being more or less modern in substance, the current consumer protection legislation in Slovenia is incomplete, incoherent, ambiguous and not user-friendly. First, there are at least two sets of laws regulating B2C contracts: CPA as *lex specialis* and CO as *lex generalis*; some of the concepts are regulated in only one of these acts, some in both, of which some are regulated similarly, and some differently. Provisions on warranty, product liability and general contractual terms as well as on sales, services contracts and package travel can, for example, be found in both acts, and it is sometimes – despite the *lex specialis derogat legi generali* doctrine – not clear which of the provisions are to be applied. This is in particularly so where the regulation of the CPA is incomplete. Further, as the CPA is basically a result of EU directives' implementation, its provisions are to be read together with the directives and their interpretation by the CJEU; this is at times difficult as some of the concepts set out in the CPA are regulated differently from the directives. In these cases, it is often not clear whether such difference is a result of improper implementation or, of the intention of the Slovenian legislator to guarantee higher protection for consumers as set out in the directives. Article 8 of Directive 1999/44 coupled with Article 3 of the Directive is a good example of this. Namely, Article 37.c of the CPA implementing Article 3 of the Directive does not set out a hierarchy of consumers' remedies as anticipated by Directive 1999/44 (and interpreted by the CJEU in *Weber & Putz*[19]). As the Directive enables Member States to grant higher protection to consumers as the one set out in the Directive, it is not clear whether in case of Article 37.c, the Slovenian legislator has in fact opted for a higher protection or it has merely overlooked Article 3 of the Directive. The outcome of such inconsistency is that the businesses, the consumers, the attorneys and the judges

[17] The time-limits are identical to those in the CPA, the hierarchy of the remedies, however, is – in contrast to the CPA – clearly set in the ZVKSES. The CPA is not applicable if the object of a sales contract is an immovable, see judgement of the Supreme Court of RS, No. II Ips 68/2012, ECLI:SI:VSRS:2014:II.IPS.68.2012. As the general regime under the CO that might be applied in all of the cases that do not fall under the CPA or the ZVKSES, sets out very strict and inflexible time-limits, it seems inappropriate that it applies to immovables. Slovenian legislation on remedies for the breach of contract should in our opinion be rewritten and various acts regulating the remedies aligned with one another.

[18] See also D. Možina, *Harmonisation of private law in Europe and the development of private law in Slovenia*, in: P. Varul (Ed.), European initiatives (CFR) and reform of civil law in new member states: international conference dedicated to the 375th anniversary of the University of Tartu, 15-16 November 2007, Juridica international, vol. 14, no. 1, 2008, Tartu, Iuridicum Foundation, 2008, pp. 173-180.

[19] Joined cases C-65/09 and C-87/09 *Gebr. Weber GmbH v Jürgen Wittmer* and *Ingrid Putz v Medianess Electronics GmbH*, judgement of 16 June 2011, ECLI:EU:C:2011:396.

are not certain how to interpret and/or apply Article 37.c of the CPA. Are the buyer's remedies set out as equal or not, is reference to the Directive and *Weber & Putz* thus at all relevant? If in the affirmative, can the provisions of the CPA be interpreted harmoniously in line with the Directive? May they be applied directly despite the horizontal relationship between the trader and the consumer or only indirectly through harmonious interpretation of Slovenian law?[20]

Even if the provisions of the CPA on the availability of the remedies are to be interpreted as granting higher protection to the consumers than the Directive and need not be interpreted in accordance with the Directive, it is not clear how they should be read taking into account that, to some extent, they differ from the general rules of the CO. Under the general contract law set out in the CO, the buyers have, in principle, the right to choose freely from any of the available remedies for breach of contract, i.e. repair, replacement, price-reduction,[21] they may also avoid the contract after giving the other party reasonable time to perform the contract. Under the CO, the objection of disproportionality is

[20] This question was relevant in the *Ribič* case dealing with the Package Travel Directive (Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tour**s,** OJ L 158, 23.6.1990, p. 59–64) where even the Supreme Court of RS struggled with the effects of the directive (see order ECLI:SI:VSRS:2015:II.IPS.160.2013).

[21] The CPA erroneously lists reimbursement of the price paid as one of the buyer's remedies instead of listing the price-reduction as a remedy (the consequence of which is reimbursement if the price already paid). Some courts have thus – in our view mistakenly – been making a differentiation between this remedy under the CO and the CPA. Such improper terminology leads also to improper application of the time-limits for bringing an action (two years after the seller had been notified of the defect by the consumer) also to unjustified enrichment claims (where the time-limit should be the general five-year limitation period). It has also not been clear in case-law and theory whether the remedy of reduction of the price is pursued out of court or only by making a claim with the court (this is particularly relevant with regard to the time-limits set out for resorting to this remedy). Some authors and judgments state that both the claim for reduction of the price and the following claim for reimbursement of the price paid should be filed with the court whereas others opine that only the reimbursement claim is to be filed with the court (in the time-limits set out for unjustified enrichment claims) whereas it suffices that the claim for the reduction of the price is made to the seller out-of-court (in two years after the seller had been notified of the defect by the consumer). See D. Možina, *Problem uveljavljanja znižanja pogodbene cene*, Pravna praksa, No. 43/2016; D. Možina, *Uveljavljanje znižanja kupnine in drugih jamčevalnih zahtevkov*, in: A. Vlahek, M. Damjan (Eds.), Pravo in politika sodobnega varstva potrošnikov,IUS Software, GV založba, Inštitut za primerjalno pravo pri Pravni fakulteti, Ljubljana, 2015, pp. 321-331, 482-483, 495; Š. Mežnar, *Uveljavljanje jamčevalnih zahtevkov za znižanje plačila po OZ in ZVPot v sodni praksi – je res potrebno razlikovanje*, in A. Vlahek, M. Damjan Pravo in politika sodobnega varstva potrošnikov,IUS Software, GV založba, Inštitut za primerjalno pravo pri Pravni fakulteti, Ljubljana, 2015, pp. 305-319, 482, 494-495; A. Galič, *Znižanje pogodbene cene – z nasprotno tožbo ali z ugovorom?*, Pravna praksa : y. 33, no. 8, pp. 9-11; see also the following decisions: judgment and order of the Supreme Court of RS, ECLI:SI:VSRS:2015:II.IPS.348.2013; judgement of the High Court in Koper, ECLI:SI:VSKP:2012:CP.1010.2011; order of the High Court in Ljubljana, ECLI:SI:VSLJ:2016:I.CP.327.2016.

available to the services provider,[22] but not to the seller.[23] However, as has been emphasized in some older Slovenian judgments, the seller may invoke at least the general principle of prohibition of abuse of right in order to deny their customer to choose a remedy that does not correspond fairly to the circumstances of the case. The CPA, too, lists the remedies of the buyer (and, in contrast to the CO, also of the services receiver) without any hierarchical order and without any explicit option for the seller or the services provider to refer to disproportionality. The general principle of prohibition of abuse of right would possibly apply here, too.[24] In contrast to the CO, however, the CPA does not even limit the right to avoid the contract by requesting the buyer to first give the seller or service provider reasonable time to perform the contract.[25] Again, it is not clear whether by omitting such rule of the CO in the CPA, the legislator intended to derogate from it or has merely forgotten about it or it perhaps intended that it applied subsidiarily. Similarly, the CPA does not provide for a provision set out in Article 3(6) of Directive 1999/44 that the consumer is not entitled to have the contract rescinded if the lack of conformity is minor. That is, however, stated in the general part of the CO[26] that explicitly applies where the CPA is silent.[27]

All three of the time-limits set out in Article 5 of the Directive (i.e. two years for the non-conformity to become apparent,[28] two months for notification and six months for the presumption) are implemented in the CPA. Additional two years' time-limit for enforcing the remedy has been added (in contrast to one year under the general rules of the CO). In contrast to Article 5(2) of the Directive, the CPA requests the consumer not only to inform the seller of the non-conformity but also to enable the seller to examine the goods what might be perceived as more burdensome to the consumer than the Directive.[29] The rule, however, seems fair under the proviso the seller covers the costs of such examination.

[22] Articles 637-640 CO.

[23] Articles 468-480 CO.

[24] See also M. Berdnik, T. Žefran, *Uveljavljanje zahtevkov v primeru napake na blagu pri čezmejnem spletnem poslovanju*, in: A. Vlahek, M. Damjan (Eds.), Varstvo potrošnikov pri spletnem poslovanju. IUS Software, GV založba, Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani, Ljubljana, 2017, pp. 33-58, 236, 244.

[25] See, for example, the following decisions of the High Court in Celje: judgement and order ECLI:SI:VSCE:2015:CP.133.2015, judgement and order ECLI:SI:VSCE:2015:CP.74.2015.

[26] Article 110 CO. It is interesting, however, that in the chapter on sales contract, the CO states that minor lack of conformity is not even deemed lack of conformity (we find this provision inappropriate).

[27] Article 37(4) CPA.

[28] One year has been added for used good whereas two years are set out for new goods.

[29] D. Možina, *Kaj je narobe z Zakonom o varstvu potrošnikov?*, Dnevi slovenskih pravnikov 2012, Podjetje in delo, y. 38, no. 6/7, GV Založba, Ljubljana, 2012, pp. 1437-1449.

One of the negative sides of the CPA is also that it did not implement Article 4 of Directive 1999/44 providing for the right of redress of the final seller against other persons in the contractual chain.

Another flaw that can be detected in Chapter VI of the CPA is that it does not implement the »IKEA clause« (nor other provisions of Article 2(5) of Directive 1999/44 according to which any lack of conformity resulting from incorrect installation of the consumer goods shall be deemed to be equivalent to lack of conformity of the goods if installation forms part of the contract of sale of the goods and the goods were installed by the seller or under his responsibility). However, the provisions of the current CPA (Article 37) might be interpreted consistent to Article 2(5) of Directive 1999/44 and the consumers may therefore possibly efficiently claim that also a defect in instructions manual resulting in defected goods is a basis for the buyers' claims.

It is clear that the Slovenian legislator has not put enough effort into introducing a clear and coherent system of remedies.[30] A more synchronized and coordinated approach to regulating consumer contracts and the system of remedies should be applied when the CPA was drafted. The CPA's inappropriate structure, language inconsistencies and substantive flaws, too, call for a reform of Slovenian consumer legislation, including the system of the buyers' remedies.[31] Also for these reasons, an entirely new CPA is currently being drafted by the Ministry of Economic Development and Technology. In August 2017, the Ministry published a draft of the new Consumer Protection Act (Sl. *Zakon o varstvu potrošnikov (ZVPot-1)*, CPA-1)[32] containing 221 Articles, a dozen of which cover the remedies for non-conformity of consumer sales contract. The draft now properly implements the "IKEA clause" as well as the right of redress of the final seller against other persons in the contractual chain. The CPA-1 continues to require the consumer not only to inform the seller of the non-conformity but also to enable the seller to examine the goods. The time-limits for the appearance of non-conformity and for notification would stay the same whereas the time in which the presumption of the seller's liability would apply, has been extended from six months to the whole period of liability for non-conformity, the provisions on the presumption have also been drafted in more detail than in the CPA

[30] For further details, see A. Vlahek, *Časovne predpostavke in vsebina zahtevkov naročnika v primeru nepravilne izpolnitve podjemne in gradbene pogodbe v slovenski ureditvi*, Pravni letopis 2012, Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani, pp. 69-83, 232-233; D. Možina, *Pravice kupca na podlagi stvarne napake pri prodajni pogodbi*, Pravni letopis 2012, Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani, pp. 85-104, 234-235.

[31] See also D. Možina (2012, *Kaj je narobe ...*).

[32] Comments to the draft could be submitted to the Ministry until 30.09.2017, http://www.mgrt.gov.si/121211211212121.1/zakonodaja_in_dokumenti/notranji_trg/predlogi_predpisov/sektor_za_varstvo_potrosnikov_in_konkurence/ (accessed on 26. 09. 2017).

and the Directive. Consumers' remedies are listed and, in contrast to the CPA, put in some hierarchical order, obviously following the provisions of the Directive (though not the *Weber & Putz* judgement) and adding further substance to them. The draft provisions state that the consumer may require that the goods are brought into conformity free of any cost (in reasonable time not exceeding 45 days[33]), or that an appropriate price reduction is made or the contract is avoided and the price already paid be returned to him or her[34]. In any case, the consumer has damages claims, in particular reimbursement of the costs for the materials, spare parts, work, carriage of goods and other costs that arise because of the consumer's remedy. A request that the goods are brought into conformity may be made unless this is impossible or such request would represent disproportionate costs for the undertaking in comparison to other consumers' remedies. The undertaking has to inform the consumer of such circumstances immediately and never exceeding 8 days after the undertaking has become aware of the circumstances. Avoidance of the sales contract is available only after the seller was given opportunity to bring the goods into conformity and did not succeed in 45 days (in some cases, avoidance may, however, be made at once: if non-conformity arises in less than 30 days after the goods were delivered or if the consumer is not entitled to request that the goods are brought into conformity). The new draft system has to some extent improved the existent regime under the CPA, but is far from perfect and not necessarily in line with the Directive and the CJEU's case-law. Additional ambiguity arises from the draft provisions on the services contract that are imprecise and in part incorrect.

Solving cases on consumer contracts is additionally difficult due to the fact that they are regulated in different acts with different provisions depending on the object of the contract, the relationship the contractual parties are, the type of the contract etc.[35] Services contract, too, is regulated in the CPA as well as in the CO whereby the two acts regulate the remedies for breach of contract differently. Additionally, the CPA does not limit the application of the rules on services contract to specific services whereas it limits the application of the rules on the sales contract to the sale of goods what additionally complicates the regulation.

What is more, an additional set of remedies (with its own hierarchy and prerequisites) in the form of a compulsory one-year warranty for new technical

[33] This time-limit has obviously been set out mirroring the one within the regime of compulsory warranty set out in the CPA.

[34] The problem here is that it ensues from the text that the claim for returning the buyer the possible price paid is to be made in the same time-limit as avoidance/price reduction claim which is erroneous in our view as the claim for returning is condictio with its own time-limits to be applied.

[35] See, for example, judgment and order of the High Court in Ljubljana, ECLI:SI:VSLJ:2012:I.CP.3269.2011.

goods, and a compulsory one-month warranty (guarantee) for used technical goods is available under Slovenian law to the buyers of specific technical goods listed in a ministerial decree.[36] Unfortunately, the consumers in Slovenia are poorly informed of the substance of the remedies available to them under both sets of rules. This is why the sellers in Slovenia often tend to mislead the consumers to believe that warranty is the only and the most advantageous instrument of their protection in case of defected goods. The reason for this lies in the regulation of remedies available to buyers under the CPA warranty scheme according to which the primary remedy for the lack of conformity is repair. Only if after 45 days the goods are not repaired, the buyer may request delivery of substitute goods.[37] If this, too, is not provided, the buyer may reduce the price or avoid the contract.[38] In recent years, ideas on the abolition of compulsory warranty in Slovenia have intensified stating that the regime restricts the fundamental freedoms guaranteed in the EU internal market, and that the competition itself would guarantee for the quality of the goods.[39] The compulsory warranty is deemed a relic of the former Yugoslav regime where it represented a form of protection of buyers of goods against the undertakings operating in central planning economy.[40]I n 2011, the first draft of the 2011 CPA amendments provided for the abolition of compulsory warranty, but the idea was later abandoned under pressure of the consumers' organizations fearing that without the compulsory warranty the buyers' rights would be too restricted. The current draft CPA-l is retaining only the voluntary type guarantee.

The problem we detect with regard to the system of the remedies under Directive 1999/44 in general is that the system of hierarchy of the remedies itself is not clear, particularly if read together with the Court's ruling in *Weber & Putz*. We believe that Article 3 of the Directive should be rewritten so as to make sure its provisions are absolutely clear and, if deemed appropriate, in line with *Weber*

[36] The CPA regulates both compulsory and voluntary guarantee (and apply not only to B2C, but also to B2B relationships). The CO also regulates voluntary guarantee making the regulation of the guarantee ambiguous. A. Vlahek (2014).

[37] The claim must be filed with the court in two years after the buyer had requested performance.

[38] A. Vlahek (2014).

[39] For a critique of compulsory warranty in Slovenia, see D. Možina, *Obvezna garancija za brezhibno delovanje in varstvo kupca v evropskem pravu*, Podjetje in delo, 1/2011, GV Založba, Ljubljana, 2011, pp. 38-48; and M. Kovač, *Garancija za brezhibno delovanje: obvezna in/ali prostovoljna*, Pravni letopis 2012, Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani, pp. 105-118, 236-237. For a proponent view, see B. Pintar, *Potrošnik in garancija za brezhibno delovanje stvari: tudi po (zdaj že umaknjenem) predlogu ZVPot-E*, Pravna praksa, 1/2011, GV Založba, pp. II-VII.

[40] For details on the evolution of the system of warranty in Yugoslavia, see M. Ilešič, *Garancija za trajno kakovost proizvoda*, Združeno delo, y. 36, no. 6 (1981), pp. 905-915. See also D. Možina (2011).

& Putz that interprets them. Possible hierarchy of the remedies should be clearly set out, (dis)proportionality of the remedies explained, the relationship between the remedy of performance of the contract and the damages liability as well as all prerequisites of these remedies should be clearly stated.[41] If the regulation of contractual damages liability falls outside the directive, it should be assessed to what extent the Member States' regulations vary and if it is possible to harmonise this aspect of contract liability, too. Only then the national legislator will have proper tools to write national legislation and the courts to apply it.

Another difficulty for the proper application of the remedies set out in Directive 1999/44 is that, surprisingly, Slovenian judges are sometimes not well familiar even with national consumer legislation, let alone with the provisions of the Directive, relevant CJEU case-law and their effects in the national legal system. The courts have sometimes even applied the CO instead of the CPA in B2C and other relationships regulated in the CPA,[42] not to mention a scandalous decision of the High Court in Maribor (sic!) upholding the first court decision stating that the rights of consumers set out in the CPA may only be pursued in administrative, and not civil proceedings.[43] Further, the courts are not well equipped with knowledge on the effects of EU directives in consumer-trader relationships. If Directive 1999/44 and corresponding CJEU case law were clear and properly implemented in Slovenian legislation, the courts would – on the proviso they would not mistakenly apply the CO instead of the CPA – surely be solving disputes as provided for in the Directive.

Question 1.2.2.

We agree that there is a need for a more comprehensive regulation of such contracts, since the use of digital content has become widespread among consumers of all ages and backgrounds and is now an integral part of the daily life in Europe. Most Member States do not yet have specific rules on supply of digital content, and national courts' attempts of legal classification of such contracts under the existing rules have thus far produced different results, which leads to discrepancies in interpretation. Due to specific characteristics of digital content, the use by analogy of the traditional rules on the sale of goods is not a satisfactory solution in our opinion. Yet it seems to be generally accepted that consumers of

[41] Assessment of contractual damages liability in Slovenia and comparative law is made in D. Možina, *Odškodninska odgovornost za kršitev pogodbe*, Podjetje in delo, 2/2016, GV založba, Ljubljana, 2016, pp. 260 ff.

[42] See, for example, the following judgments: High Court of Ljubljana, ECLI:SI:VSLJ:2011:II.CP.2207.2011; Local Court in Slovenj Gradec, No. P 248/2003 of 20 August 2009. For details on the first judgment, see D. Možina (2012, *Kaj je narobe ...*); for details on the second judgment, see A. Ferčič, *Nepošteni pogodbeni pogoji v potrošniških pogodbah*, Pravna praksa, 2010, no. 2, pp. 9-11.

[43] Order of the High Court of Maribor, ECLI:SI:VSMB:2011:I.CP.1902.2010.

digital content should enjoy the same general level of protection as consumers of tangible goods. Therefore, the regulation of contracts for the supply of digital content is a missing piece of the European consumer law. Unlike in the sale of tangible goods, borders between Member States and the geographic distance between the parties to the contract are imperceptible in the supply of digital content. This dictates the need for uniform rules for such contracts in the digital single market. Hence, the approach of maximum harmonisation is warranted. Divergence in the implementation and particularly in the application of these rules is still likely to emerge due to the fact that they will need to be applied in the context of each Member State's rules of general law of obligations. For this reason, it probably makes sense for the Directive to require Member States to create a special type of contract for the supply of digital content, distinct from sale and provision of services, in order to avoid discrepancies between national laws. This is consistent with the approach taken in the Consumer Rights Directive.[44]

We find it important that the proposal also covers contracts where digital content is not supplied in exchange for a price by against counter-performance in the form of access to consumer's personal data or other data, which are then collected by the providers in order to create value from the data processed. This business model is characteristic of a significant part of online transactions. The proposed directive is designed so that consumers under such ostensibly free contracts can also benefit from certain protections. It is important that these rules should apply also to contracts where digital content is supplied to the consumer in exchange of counter-performance in the form of other data, that is not personal data.[45]

Since the proposed directive excludes from its scope digital content which is embedded in goods in such a way that it operates as their integral part (and should therefore be legally treated as a feature of tangible goods), the concept of embedded digital content should be clearly defined and delineated from preinstalled software, to which the rules on proper digital content should apply.

Question 1.2.3.

We believe that the differences in national rules on the buyer's remedies in case of breach of a sales contract can be detected as one of the reasons (but not the

[44] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011, p. 64–88.

[45] Cf. R. Dobrovodský, *Common EU rules on digital content: future challenges for domestic legislator*, in: A. Vlahek, M. Damjan (Eds.), Varstvo potrošnikov pri spletnem poslovanju, IUS Software, GV založba, Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani, Ljubljana, 2017, pp. 83-92.

only one – there is also the problem with the language, enforcement of rights in a foreign country etc.) why the consumers and other customers do not make as much use of cross-border trade as they would have had the rules be unified and clear. The legal system as it stands now seems to be too complex for consumers and businesses to tackle with and calls for the unification of legislation at least in this area if not generally. We find a unified and unambiguous regime of the rights and obligations of contracting parties of utmost importance for establishing the trust of the businesses and the consumers in the legal order and for the proper functioning of the internal market. Any kind of additional 29th opt-in regime would (irrespective of the quality of its substance) in our view only make the system more complex and incomprehensible.[46] The same is the case if the regime is merely harmonized leaving important questions to be regulated by the Member States themselves.

Despite the positive effects a unified regime of distance selling might have on the functioning of the internal market, we are doubtful if it is wise to set out two different regimes for distance selling and regular selling. Even now, the consumers and businesses hardly tackle with the complexities of the regime of the remedies for non-conformity of the sales contract. If there were two regimes, this might lead to further ambiguity and distrust, and consequently lessening of cross-border trade. Is distance selling really that different to regular selling that it requires a completely different set of rules? We believe that a one-tier unified system should be laid down setting out only those specific rules on distance selling that are specific to this type of sale. Further fragmentation of the rules on consumer sales contract would in our opinion be detrimental to the consumers and the traders. Following the regulation set out in the Proposal for a Directive on certain aspects concerning contracts for the online and other distance sales of goods (COM(2015)635, hereinafter: the Proposal), the Slovenian draft CPA-1 has, for example, set out the two-year presumption period for all types of sale whereas so far, this period has been six months. The majority of other provisions will also be applied to both online and offline sales retaining only those specific provisions for online sales that are specific to this type of sales (pre-contractual duties, contract contents, cooling-off).

Turning to the substance of the Proposal, we believe that the system of the remedies set out in it corresponds to the one from Directive 1999/44, but are, again, not certain that the provisions can be clearly be interpreted as they were by the CJEU in *Weber & Putz*. It is our position that the provisions on the remedies of both Directive 1999/44 and the Proposal should be written in more detail (not

[46] See also A. Vlahek, *Pogodbeni prenos lastninske pravice na premičninah v evropskem pravnem prostoru*, Scientia iustitia, No. 18, GV založba, Ljubljana, 2010, 417 pp.; M. Berdnik, T. Žefran (2017).

just via the Preamble) and, first of all, the legislator should decide which system of the buyer's remedies is indeed the proper one and then set it out clearly in order to avoid any further confusion. Different from Directive 1999/44, the consumer in distance selling cases would have the right to avoid the contract also in case of minor defects. It is not clear why this should be the case in distance selling and not in regular selling. It is also not clear why under the Proposal consumers would not have the duty that they currently have under a number of national laws to notify a defect of the goods to the seller within a certain period of time from its discovery. Under the Slovenian draft of the new CPA-1 (that has been written taking into account the Proposal), these differences are not provided.

Question 1.2.4.
We do believe that enforcement of EU legislation could be strengthened for the benefit of EU consumers if a unified and unambiguous regime of the rights and obligations of the consumers and the traders is set out. However, substantive law, no matter how perfect it might be and how high the protection of the consumers it grants is, will remain a dead letter without efficient and consumer mechanisms. Although one of the key benefit of e-commerce is enabling businesses to reach wider markets, the cross-border element in consumer transactions is a barrier for the development of the internal market of the EU for various reasons, enforcement of consumers' rights outside the consumer's country and/or against a friendly enforcement foreign trader being one of them. Enforcement of consumers' rights in cross-border cases is undoubtedly more difficult that in purely national cases. Until these barriers are removed, cross-border trade will in our opinion not intensify enough even if the substantive law is unified throughout the EU.

Question 1.2.5.
What we deem most problematic with regard to online platforms is that the consumers often perceive the regular online platform providers as traders selling them the goods or services offered via the platforms, and not as mere providers of the platform services. We pose that it is important that the consumers are notified unambiguously of online platforms' role and the rights and obligations of the consumers on one hand and online platforms and the traders using he platforms on the other so as to prevent that the liabilities of both the consumer's contractual parties are not blurred in any way. As in recent years, online platforms have gained significant importance, we believe that EU consumer protection law should regulate their relationship with the consumers expressly and in more detail as the current legislation so as to cover all relevant details of the relationships between consumers, online providers and traders using online platforms. Proposals such as the Discussion Draft of a Directive on Online Intermediary

Platforms drafted by the Research group on the Law of Digital Services[47] can be a useful starting point.

Although the wording of Directive 2011/83/EC on Consumer Rights is somewhat ambiguous, it is deemed applicable also to online platform providers.[48] Online providers should provide the consumers with pre-contractual information as required by the directive, including the information on themselves and their role as intermediaries. The platform provider is the one in the position to control the information given to the consumer, whereas the seller usually has no influence on the functioning of the platform. Fines for breaching the pre-contractual duties set out in the directive should thus not be imposed on the seller who had absolutely no influence on the operation of the platform. The directive also provides for private law consequences of failing to provide the information on cooling-off, e.g., the prolongation of the cooling-off period. As the consumer can only withdraw from the contract with the seller, the seller has to bear the consequences of the platform provider's non-compliance with pre-contractual information duties. Any future legislation on platform services should address this issue, perhaps by setting out a right of redress of the seller against the platform provider. Another important question of online platform operation is the platform provider's (non-)liability for the contractual performance of the seller. In order to avoid any misperceptions on the side of consumers as to this question we believe that clear rules on this should be set out. Further obligations of online platforms can also arise from the application of legislation on unfair commercial practices and unfair contract terms. In order to address all relevant particularities of online platform operation, we believe that these, too, should be specifically covered in any novel legislation on online platforms.

Question 1.2.6.

General terms and conditions are regulated in Articles 120 and 121 of the CO while Articles 22-24 of the CPA being *lex specialis* apply for terms and conditions in consumer contracts.[49] If the terms and conditions can be qualified as unfair, then also specific Act on Consumer Protection against Unfair Commercial Practices[50] applies. There are no specific provisions on online terms and conditions set out in Slovenian legislation so the said rules apply irrespective of where these terms are available/published.

[47] Research group on the Law of Digital Services, *Discussion draft of a Directive on online intermediary platforms*, Journal of European Consumer and Market Law, Issue 4/2016, 164 ff.

[48] D. Možina, *Retail business, platform services and information duties*, EuCML 2016, 25.

[49] The draft CPA-1 regulates contractual terms in Part II, Chapter IV (Articles 21-26).

[50] Sl. *Zakon o varstvu potrošnikov pred nepoštenimi poslovnimi praksami (ZVPNPP)*, Official Gazette of RS, No. 53/07.

We have not been able to find many case-law dealing specifically with online providers' terms and conditions (be it in B2C or B2B relationships[51]). There is, however, a number of cases reported in case-law databases[52] dealing with providers' terms and conditions offline (most of them cover B2C relationships), while in some of the reported cases it is not clear whether the terms and conditions were published online or elsewhere.[53]

In one of the cases (an administrative, not a civil litigation case, where the trader sued the State and attacked the Market Inspectorate's decision finding a breach of the CPA) it was obvious that a distance sales contract was concluded (and thus the general terms and conditions were published online) as the question assessed in the case was whether the general terms and conditions were in line with the cooling-off provisions of the CPA.[54]

Online general terms and conditions were analysed also in a case assessing the legality of provisions of general terms and conditions for a car insurance but the fact that these terms and conditions were published also online, was not relevant for the assessment of the case.[55]

One of the cases dealt with online general terms and conditions in cases where a consumer sales contract was concluded via a telephone and the general terms were attached to order invoice only after the telephone conversation took place.[56] The court said that such contracts are distance sales contracts but did not assess the question of validity of the general terms as the claimant brought this argument up too late in the proceedings.

[51] For further details on the regulation of general terms and conditions in Slovenia, see A. Kaluža, *Splošni pogodbeni pogoji v evropskem in slovenskem pravu*, Master's Thesis, Pravna fakulteta Univerze v Ljubljani, 2016.

[52] www.sodisce.si; www.iusinfo.si. Judgements are available in Slovene only as only some of the key judgements of the Supreme Court of Slovenia are translated into English (http://www.sodisce.si/znanje/supreme_court_key_decisions/).

[53] See, for example, the following judgements of the Supreme Court of RS: ECLI:SI:VSRS:2011:IV.IPS.208.2010, ECLI:SI:VSRS:2008.IPS.II.158.2008, ECLI:SI:VSRS:2015:II.IPS.324.2013, ECLI:SI:VSRS:2008:II.IPS.248.2006; judgements of the Administrative Court of RS: ECLI:SI:UPRS:2010:I.U.1499.2009, ECLI:SI:UPRS:2014:II.U.296.2013, ECLI:SI:UPRS:2012:I.U.1955.2011, ECLI:SI:UPRS:2011:II.U.426.2009, ECLI:SI:UPRS:2013:I.U.1432.2012, ECLI:SI:UPRS:2013:II.U.41.2013, ECLI:SI:UPRS:2013:II.U.470.2012; judgements and/or orders of the High Court in Ljubljana: ECLI:SI:VSLJ:2012:I.CP.1214.2012, CLI:SI:VSLJ:2012:I.CP.1816.2011, ECLI:SI:VSLJ:2015:II.CP.1547.2015, ECLI:SI:VSLJ:2009:II.CP.143.2009, ECLI:SI:VSLJ:2015:II.CP.1518.2015, ECLI:SI:VSLJ:2010:II.CP.4014.2009, ECLI:SI:VSLJ:2015:II.CP.1753.2015, ECLI:SI:VSLJ:2009:I.CP.292.2009, ECLI:SI:VSLJ:2015:II.CP.1647.2015; an order and a judgement of the High Court in Maribor: ECLI:SI:VSMB:2017:I.IP.289.2017, ECLI:SI:VSMB:2017:I.CP.1344.2016; and judgements of the High Court in Celje: ECLI:SI:VSCE:2012:CP.427.2012, ECLI:SI:VSCE:2007:CP.1418.2006.

[54] Judgement of the Administrative Court of RS, ECLI:SI:UPRS:2013:I.U.1144.2012.

[55] Judgement of the High Court in Ljubljana, ECLI:SI:VSLJ:2012:I.CP.805.2012.

[56] Judgement of the High Court in Celje, ECLI:SI:VSCE:2008:CP.1315.2007.

Another case on online general terms and conditions was about general terms and conditions published on the webpage of one of Slovenian real estate agencies.[57] The agency eventually removed the problematic parts from the published general terms and conditions (on the amount of the penalty clause the consumer is to pay in specifically listed cases) but retained them in their standard contracts with their customers. The Market Inspectorate found such penalty clauses contrary to Slovenian legislation and requested to stop rendering its unlawful services until it ceases with such practice.[58] The appeal body as well as the Administrative Court of RS backed up such decision. A similar decision was rendered by the Administrative Court of RS with regard to online general terms and condition of a telecommunications services provider that were found unfair and thus contrary to the CPA.[59] The general terms and conditions stated that they the contracting parties will be informed about their eventual amendments on the internet or other reliable way. The inspectorate deemed that informing the consumer of the amendments only on the internet does not suffice (since the contract was not one on rendering internet services) whereas the court opined that such clause is not specific enough as it is not clear what »other reliable way« means.

In one of the cases the High Court in Ljubljana upheld the first instance court judgement stating that online general terms and conditions do not bind the consumer if the consumer, when concluding or attempting to conclude an offline contract (on health services), does not state that he or she will read them.[60] According to the court, mere fact that the general terms and conditions are published online does not mean that the consumer is bound by them. The consumer is bound by the general terms and conditions only if he or she was acquainted with their text before concluding the contract. The provider has to warn the consumer about them and make them available to him or her.

It is noteworthy, however, that the case-law database is covering only second and third instance judgements, having no detailed insight into the facts of the case. It is entirely unknown to what extent relevant issues have been applied by courts of first instance. Moreover, not even all second and third instance cases are published in the databases so it is possible that the relevant issues have in fact been addressed by the judiciary but are not reported.

[57] Judgement of the Administrative Court of RS, ECLI:SI:UPRS:2016:I.U.1664.2015.
[58] See also judgment of the Administrative Court of RS, ECLI:SI:UPRS:2010:I.U.1331.2009.
[59] Judgment of the Administrative Court of RS, ECLI:SI:UPRS:2014:I.U.563.2013.
[60] Judgement of the High Court in Ljubljana, ECLI:SI:VSLJ:2015:II.CP.3186.2014.

Question 1.2.7.

An initial problem in delimiting B2B from B2C relationships is the existence of various definitions of these relationships and the notion "consumer" throughout the EU and the Member States' legislations.[61] Apart from the fact that various acts of EU secondary legislation have been defining "consumer" differently (it is usually defined as any natural person who is acting for purposes which are outside his trade, business or profession,[62] but it sometimes encompasses legal persons, too[63]), some of EU directives enable the Member States to apply consumer protection legislation to other persons than those defined as consumers in the respective directives, and thus grant a higher protection also to SMEs, NGOs and other legal persons.[64]

The CPA does not define what a B2C contract (a consumer contract) is.[65] Instead, it provides for a notion of a consumer and an undertaking. A consumer

[61] See opinion of AG Cruz Villalón delivered on 23 April 2015 in Case C-110/14 *Horațiu Ovidiu Costea v SC Volksbank România SA*, ECLI:EU:C:2015:271. See also J. Cepec, *Opredelitev pojma potrošnik v pogodbenem pravu EU*, in: A. Vlahek, M. Damjan (Eds.), Pravo in politika sodobnega varstva potrošnikov, IUS Software, GV založba, Inštitut za primerjalno pravo pri Pravni fakultetiv Ljubljani, Ljubljana, 2015, pp. 111-132, 477-478, 490.

[62] See, for example, Directive 93/13 of 5 April 1993 on unfair terms in consumer contracts, OJ L 095, 21.4.1993, pp. 29-34. See also the CJEU's judgements in Joined Cases *Cape Snc proti Idealservice Srl* (C-541/99) in *Idealservice MN RE Sas proti OMAI Srl* (C-542/99), ECLI:EU:C:2001:625; and judgment in *Case Criminal proceedings against Patrice Di Pinto*, C-361/89, ECLI:EU:C:1991:118.

[63] See, for example, Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours, OJ L 158, 23.6.1990, pp. 59–64 (repealed with effect as of 1 July 2018 by Directive (EU) 2015/2302 of the European Parliament and of the Council of 25 November 2015 on package travel and linked travel arrangements, amending Regulation (EC) No 2006/2004 and Directive 2011/83/EU of the European Parliament and of the Council and repealing Council Directive 90/314/EEC, OJ L 326, 11.12.2015, pp. 1–33; Brussels I Regulation, Rome I Regulation; Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (codified version) (Text with EEA relevance), OJ L 376, 27.12.2006, pp. 21–27, and its successor; see also Green paper on unfair rading practices in the business-to-business food and non-food supply chain in Europe /* COM/2013/037 final */; Common European Sales Law (CESL); etc. In some other legal fields outside consumer protection, too, EU law grants SMEs a special status. See M. Ilešič, *Varstvo majhnih in srednje velikih podjetij v okviru potrošniškega prava*, in: A. Vlahek, M. Damjan (Eds.), Pravo in politika sodobnega varstva potrošnikov, IUS Software, GV založba, Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani, Ljubljana, 2015, pp. 133-153, 478, 490, pp. 147-149.

[64] See, for example, Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance,OJ L 304, 22.11.2011, pp. 64–88, and Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC,OJ L 271, 9.10.2002, pp. 16–24.

[65] In Article 1(1), the CPA merely states that it regulates the rights of consumers when goods and services are being offered or sold or otherwise advertised to them by undertakings, and that it regulates the obligations of state and other institutions that are to grant these rights.

is a natural person who obtains or uses goods and services for the purposes outside her professional or profitmaking activity,[66] while an undertaking is a legal or natural person performing a profit-making activity irrespective of her legal organizational or ownership status.[67] Other institutions and persons providing goods and services to consumers also have the same obligations towards the consumers.[68] It can be seen that the definitions mirror those usually set out in EU consumer directives.[69] Draft CPA-1 sets out the same definitions. A consumer is identically defined also in the Consumer Credit Act[70] and in the Act on Consumer Protection against Unfair Commercial Practices.[71]

The CO, too, does not define B2C, C2C and B2B relationships and it regulates contracts irrespective of who the parties to the contracts are. It does, however, define the meaning of a "commercial contract" to differentiate it from the so-called "civil contract" as certain concepts set out in the CO are regulated differently for commercial contracts. To name a few: regulation of statute of limitations for contractual claims; regulation of interest; regulation of assignment of claims; regulation of suretyship; relevance of business customs, usages and practice; relevance of the price determination for the validity of the sales contract; regulation of timelimits for notifying the seller of the defected goods; etc. Specific regulation of B2C contracts is not provided in the CO. Despite being the focal act regulating the law of obligations, the notions of »consumer«, »undertaking« and »consumer contract« have not been defined there. Instead, the legislator decided to define the first two in the CPA, while the definition of consumer contracts still has not been provided, but can be deducted from the definitions of the parties to the contract.

It has to be stressed, however, that there are parts of Slovenian "consumer legislation" that apply also to B2B relationships. For example, three parts of the CPA state that the rights set out in them go also to persons who are not defined as consumers by the CPA (Chapter II on product liability and Chapter IV on guarantees) or that they apply also to marketing not targeting the consumers (Chapter III on advertising of goods and services). Draft CPA-1 provides for such regime for advertising, product liability and package travel.[72]

[66] Article 1(2) CPA.

[67] Article 1(3) CPA.

[68] Article 1(4) CPA.

[69] See S. Tertnik, *Kdo je potrošnik: pojem potrošnika v pravu Evropske unije*, Podjetje in delo, 5/2012, GV založba, Ljubljana, pp. 910-922.

[70] Official Gazette of RS, No. 77/16. Strict caviats are provided in this act to protect the consumers without being clear whether they are to be applied also in cases where the natural person is aksing for a credit in order to launch its business. See J. Cepec (2015), p. 128.

[71] Official Gazette of RS, No. 53/07.

[72] The currently valid CPA does not state that for package travel which is not in line with package travel directives. See also J. Cepec (2015), pp. 128; M. Ilešič (2015), p. 138.

Extending the rules that apply to B2C relationships to B2B relationship (and, accordingly, to C2C relationships) would in some cases be welcomed in Slovenia where some of the general rules set out in the CO are very strict to the buyer and inflexible (e.g. the time-limits for the seller's liability for non-conformity which are, for example, six months after the delivery of the object of the sales contract and eight days for notification of defects (in C2C sales contract) / immediately (in B2B sales contracts as well as in cases where both parties are present at the delivery). In 2008, the Slovenian Consumers' Association and the International Institute for Consumer Studies proposed that the definition of double-purpose contract is inserted into the CPA and that it should be explicitly stated in the CPA that in cases of double-purpose contracts, a person is deemed a consumer if the purpose of business activities is so narrow that it does not dominate in the whole context of the contract.[73]

In contrast to some other jurisdictions where consumer status is given also to some legal persons (usually those contracting outside their business practices)[74] Slovenian legislation and case-law applying it do not extend consumer rights to any legal persons thus following the CJEU's interpretation of the minimal harmonisation rule of Directive 93/13 in *Idealservice*[75]. The notion of consumer is being applied narrowly as it is laid down in the CPA: a natural person who obtains or uses goods and services for the purposes outside her professional or profitmaking activity. The definition essentially corresponds to the interpretations given by the CJEU albeit it is not clear to what extent the courts pay due regard to the purpose of concluding the contracts (for personal use v. for the natural person's business) as interpreted in cases *DiPinto*, *Dietzinger, Gruber*[76] and laid down in Directive 2011/83 as well as in the CPA. There are not many cases where the question of double-purpose contracts and the relevance of the perception of the purpose of the contract by the trader was addressed by the court or cases where one of the parties was claiming that consumer protection legislation should be applied to it irrespective of its status. The Supreme Court of RS has stated that the notion of professional activity presupposes an element of durability and that thus a one-time project does not represent a professional activity although more individual contracts were concluded with different persons.[77] The

[73] J. Cepec (2015), p. 125.

[74] See J. Cepec (2015), pp. 116-119; M. Ilešič (2015), pp. 140-146.

[75] Joined Cases *Cape Snc proti Idealservice Srl* (C-541/99) in *Idealservice MN RE Sas proti OMAI Srl* (C-542/99), ECLI:EU:C:2001:625.

[76] Judgment in Case *Criminal proceedings against Patrice Di Pinto*, C-361/89, ECLI:EU:C:1991:118; judgment in Case *Bayerische Hypotheken- und Wechselbank AG v Edgard Dietzinger*, C-45/96, ECLI:EU:C:1998:111; judgment in Case *Johann Gruber v Bay Wa AG*, C-464/01, ECLI:EU:C:2005:32.

[77] Judgment of the Supreme Court of RS, ECLI:SI:VSRS:2009:II.IPS.203.2007.

Supreme Court has also held that relationships of consumer with public funds are indeed B2C relationships and both the CPA and the Act on Consumer Protection against Unfair Commercial Practices apply.[78]

Some, albeit little debate is available in Slovenian legal theory as to whether consumer protection rules should be applied to relationships outside B2C relationships in order to protect the weaker parties that are not deemed consumers. Scholars mainly present the evolution and the current status of EU legislation, CJEU's case-law, legislation and case-law of other Member States and the positions of foreign legal scholars on this issue.[79] Mojca Ilešič, though, has assessed in detail the question of protection of SMEs and stands on the position that certain higher protection of SMEs should be granted in cases where they act outside their business and where such protection would be deemed appropriate. Following the example of some other Member States, consumer protection should be extended (or a specific protection should be drafted mirroring that set out in CESL) to legal persons at least in the field of unfair contract terms.[80] We find her position persuasive.

1.3. Geo-blocking

Slovenian users of online services frequently find themselves in the position where, due to their geographic location, they cannot access online content or services that are available in other European countries. Often, they also encounter restrictions on the delivery of goods to Slovenia from online shops based in other Member States, although these seem to have significantly decreased in recent years. Of course, as a small target market, Slovenia is less attractive for large online business. Yet, this situation can be frustrating for consumers and counters the idea of the internal market. National law alone cannot adequately remedy this situation. Therefore, Slovenian consumers would surely welcome the proposed Regulation aiming to prevent unjustified discrimination on the basis of a consumer's domicile or nationality, as well as the proposal making cross-border parcel delivery more affordable and efficient.

However, the regulation should also take into account the position of small online businesses that may find it difficult to comply with all the Member States' legislation relating to any consumer in the internal market. The Commission has stressed in its Proposal for a regulation on geo-blocking (hereinafter: Proposal) that imposing additional regulatory burden on SMEs should be avoided. The Proposal therefore contains special provisions concerning the compliance

[78] J. Cepec (2015), pp. 128-129.
[79] S. Tertnik (2012); J. Cepec (2015); M. Ilešič (2015).
[80] M. Ilešič (2015).

with VAT obligations in cross-border transactions. An issue that has not been addressed in the Proposal, however, is how the prohibition of unjustified geo-blocking and other forms of discrimination on the grounds of nationality, residence or establishment will affect the application of the criterion of "directing activities to another Member State where the consumer has its domicile". This criterion is crucial for determining jurisdiction under the recast Brussels I Regulation 1215/2015[81] and also for determining the applicable law under the rules of Rome I Regulation 593/2008.[82]

The issues of the competent courts and the law applicable to their transactions might be a reasonable concern for online traders since, according to the CJEU's judgement in *Pammer* and *Hotel Alpenhof*,[83] among the evidence capable of demonstrating the existence of an activity 'directed to' the Member State of the consumer's domicile are features such as: the international nature of the activity at issue; mention of telephone numbers with the international code; use of a top-level domain name other than that of the Member State in which the trader is established or use of neutral top-level domain names such as '.com' or '.eu'; the description of itineraries from one or more other Member States to the place where the service is provided; mention of an international clientele composed of customers domiciled in various Member States and the fact that the website permits consumers to use a different language or a different currency than those generally used in the Member State from which the trader pursues its activity.[84]

We can expect that many of the listed characteristics will be applied on most online traders' websites after the adoption of the proposed regulation on geo-blocking merely to comply with the non-discrimination rules and to be able to properly serve customers from other Member States when so required. This should not be interpreted in a way that puts online traders from smaller Member States at a disadvantage compared to those from the largest Member States, for example by interpreting their use of English language as conclusive evidence of directing their commercial activities to all Member States. Whereas online businesses from larger Member States can use their own language to conduct business with customers from other Member States, the traders based in geo-

[81] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 351, 20.12.2012, p. 1–32.

[82] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177, 4.7.2008, p. 6–16

[83] Joint cases *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG* (C-585/08), and *Hotel Alpenhof GesmbH v Oliver Heller* (C-144/09), ECLI:EU:C:2010:740.

[84] A. Galič, *Mednarodna pristojnost za reševanje potrošniških sporov*, in: A. Vlahek, M. Damjan (Eds.), Pravo in politika sodobnega varstva potrošnikov, IUS Software, GV založba, Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani, Ljubljana, 2015, pp. 230-234.

graphically limited linguistic areas, such as Slovenia, are practically compelled to use a foreign language to conduct any cross-border operations. Small online traders should have a clear option of limiting the scope of their operation to the territory of a limited number of Member States, while at the same time complying with the principle of non-discrimination.

Facilitating equal online access to audiovisual content across the digital single market will also require modernisation of the EU copyright framework, since currently national laws restrict businesses from serving customers across European borders. For most businesses, geo-blocking of digital content and the modification of digital offers based on customers' place of residence within the EU are indispensable to comply with different national laws. Geo-blocking is a direct consequence of regulatory market fragmentation within the EU. Accordingly, it is not geo-blocking that hits consumers and prevents European businesses from expanding. Rather, it is legislative fragmentation of traditional sectors at the level of the national member state that imposes significant costs on businesses and consumers alike.[85]

In certain situations, of course, there are legitimate grounds for geo-blocking when ordered by the competent authorities. For example, the Slovenian Gaming Act[86] stipulates in Article 107.a that, on the proposal of the Financial Administration, the Administrative Court may order the provider of information society services to restrict access to the websites through which online gambling is organised without a government concession. The proposal must specify the extent of the restriction and the way it is to be enforced, taking into account the principle of proportionality and the technical possibilities. Restrictions on access to websites must be limited to the extent strictly necessary for the enforcement of an individual decision prohibiting online gambling and must be carried out in the least burdensome manner for the information society service provider. A draft amendment to the Electronic Communications Act presented for public discussion in July 2016 allowed (but not instructed) network operators and providers of Internet access services to block access to Internet domains listed on the Interpol's "Worst of"-list (IWOL)[87] as distributors of images of child sexual abuse. This solution was later not adopted due to the concerns of potentially disproportionate incursion into the principle of net-neutrality.

[85] M. Bauer, *Right Direction, Wrong Territory: Why the EU's Digital Single Market Raises Wrong Expectations*, American Enterprise Institute, March 2017, www.aei.org/publication/right-direction-wrong-territory-why-the-eus-digital-single-market-raises-wrong-expectations (accessed on 30. 09. 2017).

[86] Sl. *Zakon o igrah na srečo (ZIS)*, Official Gazette of RS, No. 27/95, with further amendments.

[87] www.interpol.int/en/Crime-areas/Crimes-against-children/Access-blocking/Introduction (accessed on 30. 09. 2017).

1.4. Questions related to the collaborative economy

Question 1.4.1.

Non-collaborative market players predominantly accuse their collaborative competitors of unfair behaviour in the marketplace (see Q1.4.2), although their allegations of unfair competition are rarely based on a correct legal premise.[88] As far as specific platform economy models are concerned, issues regarding taxation, administrative licencing but also labour law can be identified as chief difficulties.

Question 1.4.2.

We have so far not detected any actual *antitrust* issues in the field of sharing or collaborative economy in Slovenia. On the other hand, the representatives of the "classical" sectors of economy are extremely vocal regarding potential breaches of the *unfair competition* rules. They argue that the new, collaborative market players are ever more intensely encroaching into their respective market shares due to lack or even complete absence of any regulation (sanitary, labour, taxes) of the collaborative business model. It should be pointed out yet again that such allegations are moot without an actual or potential damage to the market participants caused by an illegal act or omission by the collaborative market players.

Question 1.4.3.

Firstly, the question should probably be either modified so that proper and exact definitions are used. It is namely not entirely clear whether the thrust of the question is aimed at (a) the so called proper *two-sided markets*, whereby the provider and controller of the platform itself *is* the service provider, (b) the *platform economies*, where platforms merely act as *information exchange providers* between two types of market players, i.e. providers and consumers, or (c) the archetypal collaborative economy model, where there are no professional platforms or professional service providers to speak of (*e.g.* car-pooling in its purest form).

Leaving this important precondition aside, it is possible to state that providing services in the market (e.g. operating a digital platform which connects suppliers and consumers for a commission) always requires one or more administrative procedures. Undoubtedly, a company or sole entrepreneur status has to be obtained according to the Companies Law to operate in the market of the Republic of Slovenia. Let us reiterate – if a natural person providing services or goods in the ambit of a collaborative economy model as a user of a platform (e.g. flat owner renting via Airbnb) is deemed to be acting in a market with the aim

[88] Unfair competition presupposes an illegal act causing or threatening to cause damage to other market participants, which cannot be inferred simply due to lack of regulation of collaborative economy and its specific nature.

of gaining profit then such a person will be deemed a business and will need to satisfy all necessary legal requirements including any and all authorisations pertaining to his/her type of services.

It can therefore be claimed that the potential necessity of authorisations and other administrative requirements for service providers in sharing economy depends on the perception of their status as a business operator.

As for the actual service providers, even those providing their services on a limited time basis and not as their main business or source of income (i.e. natural persons, which take part in the collaborative economy scheme intermittently, offering their services as a supplementary activity) are actually considered as businesses and are subject to authorisation and other administrative rules, albeit in a modified scope and breadth.

The agency that has addressed the question of collaborative economy sector the most recently was the Tax Administration of Slovenia. It has published concise instructions on procedures and requirements of business operators in the field of property rental with the aim of clarifying the most contested questions regarding fiscal (tax) obligations of such operators. The instructions and the regulation therein are aimed at providers of lodging services (renting room, flats, houses etc.) in cases where their provision of services is a limited one. The lodgings have to be provided for a limited time (no longer than 5 months a year) and in with a maximum capacity of 15 beds, while the list of prerequisite permissions and other requirements is quite ample, consisting of:

- Proof of ownership of the immovable used for provision of services
- Operating permit for certain types of lodgings (depending on the year of construction)
- Consent of co-owners, in the case of a multi-apartment building the provider has to obtain the consent of *all* co-owners.
- Living conditions in the lodgings have to satisfy the standards provided for by the Rules on categorization of the accommodation facilities
- Special conditions provided for by the Rules on minimal technical requirements and on the scope of services for hospitality operations[89]

Question 1.4.4.
Please see answers to question 1.2.1.

Question 1.4.5.
The answer depends on the type of the service provided, the meaning of the term trader, and the type of the platform operator. In all platform economy sectors a

[89] Sl. *Pravilnik o minimalnih tehničnih pogojih in o obsegu storitev za opravljanje gostinske dejavnosti* (Official Gazette of RS, Nos. 21/14 and 35/17)

three-party contractual relation develops due to the phenomenological characteristics of two-side markets. The underlying presumption of peer-to-peer economies (i.e. collaborative or sharing economies) is the concept of peers sharing their goods or services eith other peer "consumers" without a transfer of property rights, whereby the intermediaries are the operators of platforms aiding in transactions between peers. The question of designation of any of those parties in collaborative transactions as "traders" is important mainly because it establishes (or better, changes) the position of such parties in light of their potential liability for damages and, in addition, their position as far as administrative and taxation requirements are concerned As already mentioned above (see Q1.4.3), providing services in the market (e.g. operating a digital platform which connects suppliers and consumers for a commission) always requires one or more administrative procedures. Undoubtedly, a company or sole entrepreneur status has to be obtained according to the Companies Law to operate in the market of the Republic of Slovenia. Let us reiterate – if a natural person providing services or goods in the ambit of a collaborative economy model as a user of a platform (e.g. flat owner renting via Airbnb) is deemed to be acting in a market with the aim of gaining profit then such a person will be deemed a business and will need to satisfy all necessary legal requirements including any and all authorisations pertaining to his/her type of services.

Question 1.4.6.

In our opinion, collaborative economy markets should remain as open and non-regulated. Extensive regulation and establishing of new concepts of consumer protection could lead to the demise of real platform economies, as, firstly, platform operators would gradually have to transform into virtual service providers (as their liability would broaden and encompass the damages arising from the provision of service itself). Secondly, there is a concern that peers would start morphing into "actual" service providers as their status changes due to higher levels of scrutiny and liability. We are therefore of the opinion that softer measures in the form of trust-building mechanism, score reports and score sheets etc. are indeed more appropriate for the task at hand. The level of information asymmetry that undoubtedly exists in platform economies can also be lowered by self-regulatory measures by the peer-providers. Establishing, enacting best practices codes and abiding by such codes could absolutely carry an important message to the consumers. Generally, we believe that intense competition and consumer protection mechanisms in place at he moment together with the aforementioned "soft instruments", i.e. scoring, labelling, shaming, are sufficient to build the confidence in providers that deserve it.

2. Digital media

Question 2.1.
After having consulted the annual reports and other documents published by the AKOS (national regulatory agency), we have unfortunately not been able to identify any Slovenia-specific established practice pertaining to the issue at hand. We do, however, feel the need to express our doubts regarding the judgment of the Court in the *New Media Online* case as we are of the opinion that even in the conditions of optimal convergence, the primary, original nature and form of the media (and not the nature and specifics of the technological means that the medium uses to reach its consumers) should be taken into account when deciding upon potential application of the AVMS Directive regime.

Question 2.2.
We believe such a proposal to be extremely problematic especially in the field of platforms that do or could encourage user-generated content. Adding to paradoxically backward copyright law already in place, intensive regulation reaching from protection of minors to commercial communication could further thwart independent creative forces striving to craft what can be called "read-write" culture and do not adhere to the policy of simple (inconspicuous) consumption of industry generated artefacts of mass-produced "culture". Therein also lies the most inherent danger of the "single digital market" concept as it follows the industry-created idea of commodization of culture. At the time of conclusion of this report, no national legislation providing for sector-specific rules for AV platforms was in place in Slovenia.

Question 2.3.
We have not identified any of the above problems at the time of finishing this report. As per the national regulatory Agency (AKOS) annual reports, the only time the regulator has intervened with the AVMS providers established in other Member States was on the issues regarding the amount of per-hour advertising programmes.

Question 2.4.
The regulation of the media landscape in Slovenia is somewhat balkanized. The field is regulated and controlled by multiple institutions, their powers and jurisdiction set forth in at least three separate Acts. The Agency for Communication Networks and Services of the Republic of Slovenia[90] – an independent institution – regulates and supervises the electronic communications market, manages

[90] Sl. *Agencija za komunikacijska omrežja in storitve Republike Slovenije (AKOS)*.

and supervises the radio frequency spectrum in the Republic of Slovenia and performs tasks in the field of radio and television broadcasting. As it is a public agency, its status is that of complete independence and neutrality as regards the government of the Republic of Slovenia. Its main media regulation tasks are (a) the supervision and active control of the rules on minor content, (b) ensuring the protection of public interests regarding program content and providing equal conditions for operations of radio and television program publishers and other audiovisual content providers by expertly supervising the implementation of the program requirements and restrictions that apply to radio and television programs and the obligations of other audiovisual content providers, (c) control of shares of in-house production and shares of audiovisual work from Slovenian and European producers, (d) control over adherence to limitations for broadcasting advertising content, (e) control over program requirements and limitations arising from licenses for conducting radio or television activities. In addition, the Broadcasting Council of the Republic of Slovenia[91] acts as an independent expert body in the field of broadcasting regulation. Its tasks and powers are, *inter alia*:

- it shall provide the Agency for Communication Networks and Services of the Republic of Slovenia with initiatives for the conduct of expert supervision of the implementation of programming requirements and restrictions specified in the present act and shall adopt the annual plan for the conduct of such supervision
- it shall adopt decisions on the issue, revocation and transfer of licences for performing radio and television activities, and provide the agency with binding proposals and approvals for the issue and revocation of licences for performing radio and television activities
- it shall adopt decisions on the assignment or revocation of the status of a local, regional or student radio or television station, and propose to the agency the issue of the relevant acts
- it shall provide the relevant ministry with a preliminary opinion on the assignment or revocation of the status of a non-profit radio or television station
- it shall adopt decisions for the preliminary opinion of the agency in connection with the restriction of concentration
- it shall propose to the responsible minister detailed criteria for defining local and regional programming, the procedure and conditions for acquiring the status of special stations, and criteria for in-house production and other programming on radio and television stations specified in the present act

[91] Sl. *Svet za radiodifuzijo Republike Slovenije (SRDF)*.

- it shall give approval to regulations setting out the procedure for issuing, amending, renewing and revoking the licence for performing radio and television activities and the content of the ruling on the issue thereof.

According to Article 56 et seq. of the Mass Media Act of 2006, The Ministry of Culture adopts and issues potential consent decrees regarding a referred acquisition of an ownership or a management stake or a share in the capital of a publisher of a radio or television station or daily informative printed medium of twenty per cent or more. Prior to its decision, the Ministry is to acquire official opinions regarding such a concentration from the Broadcasting Council and The Agency for Communication Networks and Services.

We do not see a potential specific benefit in harmonization or unification of independence requirement for the national media regulators in the future if such a requirement can be satisfied through declaratory means of legislation. Looking at the case of Slovenia, one can detect cases (e.g. the Agency for Protection of Competition) where an authority has been granted full independence by the law, while its budgetary requirements are decided by a Ministry, thereby stripping the Agency of its actual independence. As for the potential political or commercial pressure we have no robust data attesting to such pressure being exerted systematically.

Question 2.5.

The most contentious issues in the field of broadcasting laws and regulation in the past twenty years were undoubtedly (a) the controversy surrounding the constitutionality of reply[92], (b) the role of the national public television[93] and, lately, (c) questions pertaining to media plurality, more precisely the role of certain institutions (namely the Ministry of Culture) regarding the issuance of consent decrees. We do not believe that further harmonisation of any of the mentioned areas of interest through the AVMS or other directives would result in considerably beneficial outcomes, as the said issues mainly stem from the lack of political culture and (at least in Slovenia) certain irreconcilable historical differences. The only area that might benefit from further harmonisation is that of media concentration, where the strengthening of independent national media regulators could improve the current status of media plurality.

[92] For further reading regarding this issue, please consult Krivic, Zatler: *Svoboda tiska in pravice posameznika*, Open Society Slovenia, Ljubljana, 2000, http://mediawatch.mirovni-institut.si/edicija/seznam/06/mediawatch06.pdf (accessed on 30. 09. 2017).

[93] The role and future of the Radio Television Slovenia (RTVSlo) has been hotly debated since the independence of Slovenia in 1991, whereby the main issue can be summarised as the question of level of involvement (or better – control) of the political parties in the management of the public broadcaster and their influence (direct or indirect) over the programme content, especially the daily news.

Question 2.6.
At the time of writing of this report, no such initiatives were detected in Slovenia. Due to the extremely pervasive nature of the television medium we strongly believe that target or addressable advertising definitely is in need of a EU-wide harmonised approach. We would advise extreme caution, as in our opinion this type of advertising is capable of significantly impacting (and in final stages – changing) consumer preferences.

Question 2.7.
The specific regime tor TV and radio broadcasting by satellite and cable is still of importance in Slovenia. We are unaware of any specific systematic rules on licencing that would similarly apply to online transmissions by broadcasters. It is worth mentioning, however, that the recently adopted Collective Management of Copyright and Related Rights Act excluded making copyrighted works available to the public from the ambit of collective management,

Question 2.8.
We have thus far not detected any *special* barriers that could prevent the effectiveness of the cross-border portability of content in Slovenia. This is not to say, however, that the concept will not collide with the same problems that will undoubtedly arise in other member states. Cross-border portability, akin to the issue of geo-blocking, which intrinsically hampers the freedom of IP owners to apply geographical non-price and price discrimination, interferes with the absoluteness of the copyright enjoyed by its owner. In addition, Slovenian copyright owners warn of potential adverse effects of the economic power asymmetry between the rights holders and service providers, and fear that, given the market power of some service providers, many European rights-holders will be compelled to apply the waiver clause and authorise portability of their content without verification of the Member State of residence. In their opinion[94], some means of verification of the Member State of residence (such as the credit card number of the subscriber) are not adequate.

3. Digital infrastructures

Question 3.1.
Yes, Slovenia was the second EU Member State, after the Netherlands, to introduce net neutrality rules in its legislation, which occurred in 2012, before the adoption of Regulation (EU) 2015/2120. The new Electronic Communications

[94] *"Luknje" v predlogu uredbe o zagotavljanju čezmejne prenosljivosti*, www.aipa.si, 24.2.2017 (accessed on 30. 09. 2017).

Act (ECA)[95] of 2012 defines net neutrality in Article 3 as the principle by which all internet traffic on a public communications network is treated equally irrespective of content, application, service, equipment, source and purpose of communication.[96] Article 203 ECA further defines the objectives that the Agency for Communication Networks and Services of the Republic of Slovenia should follow when carrying out its competences in this field. Paragraphs 1 and 2 provide that the Agency shall promote the preservation of the open and neutral character of the internet and the possibility of end-users making their own choices with regard to access, the dissemination of information or the use of applications and services. The main operative provision on net neutrality is contained in paragraph 3 under which network operators and internet service providers must make every effort to preserve the open and neutral character of the internet such that they do not hinder, withhold or slow down internet traffic at the level of individual services or applications, or take measures to degrade these services or applications, except in the event of:

1. urgent technical measures to secure the undisturbed operation of networks and services (e.g. avoidance of network congestion);urgent measures to preserve the integrity and security of networks and services (e.g. removal of undue excessive load on a transmission medium/channel);
2. urgent measures to restrict unsolicited communications under Article 158 of this Act; or
3. a court decision.

The measures under points 1, 2 and 3 must be proportionate, non-discriminatory, subject to a time-limit and carried out to the extent necessary to achieve their objectives.

Paragraph 5 further stipulated that services provided by network operators and internet service providers may not be based on services or applications offered or used via internet access services. The official explanation in the draft law stated that this provision meant that it is not allowed to provide internet access services limited to only parts of the Internet, which would allow access only to certain websites, services or applications (e.g., e-government, e-health), while others are blocked or differently priced.[97] This provision, together with the definition of net neutrality principle in Article 3 was relied upon by the Agency when adopt-

[95] Sl. *Zakon o elektronskih komunikacijah (ZEKom-1)*, Official Gazette RS, No. 109/12 with further amendments.

[96] See B. Makarovič, *Novi Zakon o elektronskih komunikacijah – Po domače začinjen regulativni okvir EU*, Pravna praksa, 2012, No. 45, p. 8.

[97] Sl. *Predlog Zakona o elektronskih komunikacijah za prvo obravnavo*, EVA 2012-3330-0058, 28.09.2012.

ing the position that zero-rating also violated net neutrality. It is worth noting, however, that the draft ECA proposal from 2012 originally envisaged a more explicit prohibition of price discrimination, since paragraph 5 contained an additional sentence stipulating that individual services or applications provided or used through internet access services should not affect the price of services of network operators and internet access providers. The National Assembly's Committee on Education, Science, Culture, Sport and Youth decided to delete this sentence due to concerns of its disproportionality.[98]

After the adoption of Regulation (EU) 2015/2120, in order to avoid any duplication or collision with its provisions, ECA was amended in 2017, taking into account, *inter alia*, specialised services foreseen in the Regulation as an exception from the net neutrality principle. Points 1 and 2 in paragraph 3, Article 203 ECA were deleted since these exceptions from the net neutrality principle are already contained in provisions of Article 3(3)(b) and (c) of the Regulation. Instead, a new provision was inserted, which allows the operators to temporarily deviate from net neutrality when carrying out emergency measures in the event of extraordinary situations in accordance with Article 83 ECA. This covers the operators' obligation to give priority to the operation of those parts of the network required for the continuity of operation of the networks of entities responsible for the security and defence system and the protection and rescue system. Paragraph 5 of Article 203 ECA was also deleted on the grounds that a legal prohibition of zero-rating would be contrary to Regulation (EU) 2015/2120, which does not prohibit this practice *a priori*.[99] This should not be taken to mean that zero-rating is now considered compatible with the net neutrality principle, but rather that the interpretation of this is left to the Agency and the courts.

In 2015, the Agency carried out five inspection procedures against mobile operators as internet access providers (including Telekom Slovenije and Si.mobil, the two largest operators in Slovenia), due to the suspicion of violation of Article 203 ECA, since they offered to end users several own services without charging for data transfer on the operator's network. The zero-rated internet traffic, which was excluded from the monthly amount of data transfer, included free music streaming, free cloud storage service, free TV on mobile devices and free access to certain other operator's applications and services. In all cases, the operators were found guilty of violating net neutrality principle by economically discriminating against other traffic to give their own zero-rated services priority. The operators argued that net neutrality as regulated in Slovenian ECA only referred to technical issues of providing internet access to end users, and not

[98] Ibid.

[99] Sl. *Predlog zakona o spremembah in dopolnitvah Zakona o elektronskih komunikacijah za prvo obravnavo*, EVA: 2016-3130-0038, 12.04.2017.

to price discrimination by offering zero-rated services, since this was not specifically mentioned in the law. The Agency did not accept this reasoning and held that, due to the definition of net neutrality in Article 3 ECA, the prohibition does not cover only technical means like hindering, withholding or slowing down internet traffic, but also any other measure that would degrade other services or applications, including price differentiation. The Agency instructed operators with regulatory decisions to treat all internet traffic equally in such a way that every user in their mobile network is charged for it fully and independently of the type of service, application, or content in connection with which the internet traffic occurred.[100]

However, the operators contested these decisions and in July 2016, Administrative Court reversed the Agency's decisions and remanded the cases to the Agency for repeated proceedings. The court held that the provisions of paragraphs 3 and 5 of Article 203 ECA cannot be interpreted in the sense that they prohibit any economic differentiation between internet access services depending on the use of the service or application. The court found no clear grounds in the wording of the law to include in the net neutrality principle the prohibition of price discrimination in terms of different charging for data traffic depending on the service or application used.[101] These judgements were criticised by some experts for too superficial reasoning without any substantial discussion of the issues of net neutrality as technical and commercial conditions of internet access are often intertwined and cannot be treated separately. However, a part of the blame was also attributed to the Agency, which failed to issue a general act regulating in more detail the implementation of the provisions on net neutrality.[102]

Another possible violation of the net neutrality principle was detected by the Electronic Communications Council of Slovenia, which noted that network operators and internet access service providers in their terms of service prohibit or limit the shared use of internet connection established via a mobile phone or other mobile terminal device (tethering). The Council called on the Agency to act accordingly.[103] However, the Agency took the view that this is not a case of limiting the use of internet connection at the level of a specific service or an application, but at the level of a device, which is not covered by the net neutrality

[100] The decisions Nos. 06101-37/2015/7, 06101-1413/2014-4, 06101-1412/2014-4, 06101-813/2014-4 and 06101-747/2014-4 are available at the Agency's website: http://www.akos-rs.si/odlocbe-po-inspekcijskem-postopku.

[101] Judgements of the Administrative Court of RS, ECLI:SI:UPRS:2016:I.U.295.2015 and ECLI:SI:UPRS:2016:I.U.1350.2015.

[102] D. Caf, *Igranje z ugledom in razvojem države*, Delo, 25. 08. 2016, http://www.delo.si/mnenja/gostujoce-pero/igranje-z-ugledom-in-razvojem-drzave.html (accessed on 30. 09. 2017).

[103] Opinion of the Electronic Communication Council of 29. 1. 2016, http://www.sek-rs.si/Portals/0/Content/Datoteke/Mnenja/SEK(2016)-03%20Nevtralnost%20interneta.pdf (accessed on 30. 09. 2017).

principle under ECA. The Agency hinted, nevertheless, that contractual limitation of tethering could be contrary to the rules of the Regulation (EU) 2015/2120, which was not yet in force at the time and which proscribes equal treatment of all data traffic, irrespective of, *inter alia*, the terminal equipment used.[104]

Question 3.2.

We have detected no particular need nor desire among Slovenian telecommunication service providers for the introduction of EU-wide licensing schemes in the field of telecommunications.

In order to transpose Directive 2014/61/EU on measures to reduce the cost of deploying high-speed electronic communications networks, twelve national legislative acts were amended, among them Electronic Communications Act, Law on Motorway Company in the Republic of Slovenia, Spatial Planning Act, Roads Act and Construction Act. Due to the delay in transposition of this directive, the European Commission delivered, in September 2016, a reasoned opinion under Article 258 TFEU on Slovenia's failure to fulfil its obligations. The Government replied in March 2017 that the full transposition of the directive in Slovenian legal order would be completed with the adoption of amendments to the Electronic Communications Act. This happened in July 2017.

One of the measures foreseen in the Slovenian Development strategy for the information society until 2020 to promote broadband infrastructure is the provision of additional segments in the radio spectrum for mobile communication networks to provide mobile access to the internet as a complementary communication service to fixed broadband infrastructure.[105]

Question 3.3.

The European regulatory framework of 2009 introduced, among other things, a more modern way of managing radio frequencies for electronic communications: among the basic principles are non-discrimination, objectivity and transparency of frequency allocation, technological and service neutrality of use of radio frequency bands. However, the practical implementation of these principles was delayed in Slovenia, since Electronic Communications Act of 2012 allowed the Agency to simply extend the validity of a decision allocating radio frequencies for the provision of public communications services to end-users (that would normally expire in 2013), up to 25 May 2016. This kind of grandfathering of spectrum rights was criticised in legal literature as potentially unconstitutional.[106]

[104] http://www.resimo.net/index.php/2015/12/23/akos-telekomov-tethering-je-v-skladu-z-zakonodajo (accessed on 30. 09. 2017).

[105] *Digital Slovenia 2020 – Development strategy for the information society until 2020*, March 2016, p. 27.

[106] B. Makarovič (2012), p. 8.

The Supreme Court confirmed that no public tender was required to extend the validity of existing licences, but that licence holders had to pay an additional fee for the extended period, set by the Agency in accordance with criteria set out in Article 60 ECA.[107]

Republic of Slovenia has difficulties in the international coordination of the radio frequency spectrum with Republic of Italy, where radio and television stations broadcast on frequencies for which Slovenia did not give consent have appeared since the mid-1980s. According to the available data, Italy did not coordinate internationally new radio stations, but simply issued them licences to use frequencies that were free at the time. This led to the situation where Italian radio stations are being broadcast in the vicinity of the Slovenian border on frequencies already broadcast by Slovenian radio stations or on frequencies that were awarded to the Republic of Slovenia by international agreements, which is illegal according to International Telecommunication Union's Radio Regulations. On the basis of complaints from Slovene broadcasters of television and radio programs and on the basis of their own measurements, the Slovenian Agency repeatedly reported to Italy the disruptions caused by stations on its territory.[108] This situation was partially rectified in 2016, after Italy switched off television broadcasting transmissions on 61 frequencies which had been causing harmful interference into television broadcasting services of neighbouring countries.[109] However, interferences between radio frequencies allotted to radio stations remain and have led to several lawsuits being filed by Italian radio stations against Slovenian radio stations broadcasting on the same frequencies.[110]

Question 3.4.

The Slovenian national regulator in the field of electronic communications is Agency for Communication Networks and Services of the Republic of Slovenia, which is set out in the legislation as an independent body that regulates and supervises the electronic communications market, manages and supervises the radio frequency spectrum in the Republic of Slovenia, performs tasks in the field of radio and television broadcasting, and regulates and supervises the postal and railway service markets.[111]

[107] Judgement of the Supreme Court of RS, ECLI:SI:VSRS:2015:X.IPS.117.2014.

[108] M. Pohar, I. Funa, *Posledice nekoordinirane rabe radijskih frekvenc med državami*, Pravna praksa, 2015, No. 24-25, p. 28.

[109] *Italy Switches Off Harmful Frequency Transmissions,* Geneva, 30 November 2016, http://www.itu.int/en/mediacentre/Pages/2016-PR58.aspx (accessed on 30. 09 .2017).

[110] *Italijanske radijske postaje nadaljujejo motenje in tožbe*, 23 April 2017, https://www.rtvslo.si/slovenija/italijanske-radijske-postaje-nadaljujejo-motenje-in-tozbe/420551 (accessed on 30. 09. 2017).

[111] http://www.akos-rs.si/about-akos.

The bodies of the Agency are the Agency Council and the Agency director. The Council has no decision-making competences on regulatory issues were the Director acts independently. The Council, however, gives opinions on the work programmes, the financial plan and the annual report and may suggest improvements and point out irregularities. The members of the Agency Council and the director are appointed by the Government on the basis of a public tender by the Ministry for a fixed term of five years, which is renewable after holding a public tender. The law secures their impartiality by listing various circumstances that are incompatible with the functions, such as stock ownership in legal entities active in an area which the Agency is competent to regulate. The Government may dismiss the director and members of the Agency Council before the end of their term of office only in circumstances stipulated in the law.

Article ECA specifically guards the Agency's independence of operation in regard of ensuring competition, by providing that in implementing these tasks, the Agency may not request or receive instructions from any other state bodies. However, this should not preclude it from consulting the body responsible for competition protection nor from cooperating with other regulatory authorities, the European Commission or BEREC.

Despite the Agency's structural and operational independence, concerns have been expressed that the independence may be threatened if the body lacks staff and financial resources.[112] The consent to the Program of Work and Financial Plan of the Agency must be made by the Government. As long as the Government does not give its consent, which happened in 2013, the Agency does not have guaranteed stable funding, and consequently cannot carry out the necessary training and recruitment of professional staff due to the key projects of the Agency. [113]

There have been no legal challenges in relation to the independence of the Agency.

4. Data in the digital economy[114]

Question 4.1.

The General Data Protection Regulation (GDPR)[115] entered into force on 25 May 2016 and will become directly applicable in all Member States two years after

[112] T. Jernejčič, *Nevtralnost interneta s posebnim ozirom na zero-rating storitve,* Master's thesis, Ljubljana, 2016, pp. 32–33.

[113] AKOS Annual Report for 2014, http://www.akos-rs.si/letno-porocilo-2014.

[114] We would like to thank Mr. Peter Pavlin of Ministry of Justice of RS for his valuable contribution to this topic.

[115] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

its publication. The same deadline also applies for transposition of Directive 2016/680 on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities[116] into national law. In Slovenia, the project of implementing these acts has been led by the Ministry of Justice that is competent for drafting personal data protection legislation. On 4 October 2017, the Ministry published a Draft Proposal of the new Personal Data Protection Act (Sl. *Zakon o varstvu osebnih podatkov (ZVOP-2)*)[117]). This new act will replace the existent Personal Data Protection Act (Sl. *Zakon o varstvu osebnih podatkov (ZVOP-1)*) of 2004 that entered into force on 1 January 2005. Before that, the Personal Data Protection Act (Sl. *Zakon o varstvu osebnih podatkov (ZVOP)*) of 1999 applied.

In its brief news, the Ministry of Justice of the Republic of Slovenia stated that observing the provisions of the GDPR and Directive 2016/680, the new draft proposal sets out anew the objectives of processing of personal data, legal grounds for processing of personal data, use of information society services by children, data controllers, codes of conduct with personal data etc.[118] The draft proposal pays due regard to the balance between various constitutional rights, i.e. the right to protection of personal data on one side, and other rights, such as the right to free speech and the right of access to public information, on the other. The draft proposal follows the current regulation according to which the Information Commissioner of the Republic of Slovenia (Sl. *Informacijski pooblaščenec*)[119] is the national data protection supervisory body for all cases of processing personal data (with some exceptions arising from the GDPR or similar Slovenian legislation).[120]

Already during the legislative process of the GDPR, Slovenia was emphasizing that primary goal of the new regime should be to preserve the high level of personal data protection and that it is vital that the regulation has clear and consistent provisions.[121] According to the Ministry, EU members are likely to

[116] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[117] The text of the draft is available here (in Slovene only): http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/mp.gov.si/novice/2017/september_2017/171004_ZVOP-2_status.pdf (accessed on 5. 10. 2017).

[118] http://www.mp.gov.si/si/medijsko_sredisce/novica/article/12447/7469/ (accessed on 5. 10. 2017).

[119] https://www.ip-rs.si/en/ (accessed on 29. 11. 2017).

[120] Ibid.

[121] http://www.vlada.si/en/media_room/newsletter/slovenia_weekly/news/article/commissioner_jourova_in_slovenia_also_on_reform_of_the_slovenian_judiciary_54373/ (accessed on 5. 10. 2017).

face several challenges when implementing the new regulation as, although it contains many compromises and provides possible solutions, a number of ambiguities remain. For example, there were concerns in Slovenia that the new regulation could result in the lowering of human rights standards already in place. Attention was drawn to Article 25 "Data protection by design and by default", where the Ministry has argued that there was a lack of clarity on the stated provisions for scientific research.[122] In order to achieve legal clarity of the national implementing legislation, Slovenia`s aims in drafting the proposal were to draft the provisions as exact and clear as possible. As the GDPR is a rather complex legal act, the ministry wished to make the implementing act easily applicable for use by ordinary data subjects (user friendly approach). The Ministry also aimed at resolving in this draft proposal certain legislative issues of how to implement the »directive oriented« provisions of the GDPR, as well as the similar rules from the accompanying Directive 2016/680**.** It has been emphasized that drafting the implementation provisions of these acts is rather complex and challenging.[123] When publishing the draft proposal, some of its provisions have not been finalized and the Ministry has set out various versions of such provisions hoping that during the public consultation the final text of these provisions can be drafted.[124]

The draft proposal was in the public consultation process until 13 November 2017 and is, at the time of writing this report, being polished by the Ministry of Justice that has stated that it would consult also the Information Commissioner as well as other Member States that have already drafted their implementing legislation. It is claimed that this will plausibly be the only implementing act as other existent relevant acts already conform to the two EU acts.[125] The final text of the Proposal is to be finalized by the Ministry of Justice by the end of November 2017 and then submitted to the Government of the Republic of Slovenia in adoption and submission to the Slovenian parliament.

Question 4.2.

At the moment we can assess that the Information Commissioner of the Republic of Slovenia is sufficiently prepared for the application of the novel rules expertise wise. It has been focusing on the substance of the new rules of data protec-

[122] https://www.ip-rs.si/en/legislation/general-data-protection-regulation/ (accessed on 30. 9. 2017).

[123] https://www.dataprotection-officer.com/index.php?route=blog/article&blog_post=49&create_pdf=true (accessed on 5. 10. 2017).

[124] https://www.dataprotection-officer.com/index.php?route=blog/article&blog_post=49&create_pdf=true (accessed on 5. 10. 2017).

[125] https://www.dataprotection-officer.com/index.php?route=blog/article&blog_post=49&create_pdf=true (accessed on 5. 10. 2017).

tion, publishing information on the topic and taking part in various conferences covering the GDPR and the accompanying Directive. Slovenia has also provided additional finances for new employments at this independent body and additional (significant) work space for its new supervisory operations as required under the new rules.

On the other hand, the Ministry of Justice detects that Slovenian data subjects, data controllers, companies in general and public authorities, are only starting to prepare for the application of new rules. There is, however, surely a difference in the intensity of mastering the new rules between international companies and SMS companies. The companies in general have started educating themselves in this field and participate in seminars, workshops,[126] read available literature and cooperate with the Information Commissioner in order to receive feedback to their questions relating to the new rules.[127] Unless they already employ such persons, the companies have started looking for free-lancers as their DPOs. Some data protection specialists have also started offering such services and are organizing conferences and workshops to inform the companies of their future obligations under the new rules and to promote their services.[128]

Question 4.3.

In brief, the following positions are held by the Republic of Slovenia concerning the Internet of Things (IoT) and similar processing operations, like Big Data and AI in connection with the GDPR and national implementing legislation:

- strict (guarantist) approaches to unique national identifiers and also concerning any interconnections/inter-linking that is performed by their use;
- tracing of all processing(s) of personal data;
- special strict (guarantist) provisions on interconnections/inter-linking;
- respect for the principle of finality (primary purpose of processing of personal data);
- strict (guarantist) approach towards the processing of personal data for other (secondary) purposes.

These positions arise from the strict interpretation of Article 38 of the Constitution of the Republic of Slovenia (right to personal data protection) as provided by the Constitutional Court of the Republic of Slovenia in its settled case-law

[126] See, for example, http://www.amcham.si/en/-general-data-protection-regulation-gdpr-should-become.html (accessed on 5. 10. 2017).

[127] See, for example, https://www.ip-rs.si/vop/spletne-storitve-in-gdpr-2983/; https://www.ip-rs.si/vop/gdpr-pravica-do-pozabe-in-mala-podjetja-2910/ (accessed on 29. 11. 2017).

[128] See, for example, https://www.dataprotection-officer.com/ (accessed on 29. 11. 2017).

since 1992. Slovenia`s special experience as of 2003 (the »Affair udba.net«[129]) has also contributed to the strict interpretation of relevant provisions. It is to be added that Slovenia intervened on behalf of the Claimant in the CJEU *Schrems* case[130] concerning Facebook and Safe Harbour Agreement concluded between the USA and the EU.

Question 4.4.

In Slovenia, the administrative and court practice on this issue is scarce. The Information Commissioner has issued several (non-binding) opinions in delisting request cases in which the Commissioner is referring to the Google Spain case.[131] There are, however, no publicly available court decisions dealing with this issue.[132] It is thus yet to be seen how the courts will apply the rules as interpreted by the CJEU. According to Google Transparency Report, requests for 6776 ULRs were received from Slovenia from the date the request form had been launched by Google (29 May 2014) until 1 December 2017. In 33,4 % of the cases, the URL were removed by Google.[133] The majority of the requests is supposedly submitted by private persons.[134]

There is some legal literature on the *Google Spain* case which presents the substance of the CJEU case and its consequences for national institutions.[135] One of the articles has also presented the guidelines on the delisting issued by

[129] See, for example, B. Makarovič, *Foreign Internet content restriction in the Republic of Slovenia: Artificial borders within the Internet to protect personal data?*, Journal of Computer, Media and Telecommunications Law, Volume 8, Number 5, 2003, pp. 371-374.

[130] Judgment in Case *Maximillian Schrems proti Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.

[131] See, for example, https://www.ip-rs.si/vop/pritozba-zoper-zavrnitev-zahtevka-za-umik-rezultatov-iskanja-po-google-2363; https://www.ip-rs.si/vop/izbris-povezav-o-fizicni-osebi-v-zvezi-s-kaznivimi-dejanji-2962/; https://www.ip-rs.si/vop/odstranitev-ze-umaknjene-slike-iz-google-images-indeksa-2450/; https://www.ip-rs.si/vop/objava-kriminalne-preteklosti-posameznika-na-spletu-2446/; https://www.ip-rs.si/vop/umik-povezav-do-strokovnih-clankov-iz-rezultatov-iskanja-po-osebnem-imenu-2438/ (all accessed on 5. 10. 2017).

[132] www.sodisce.si.

[133] See https://transparencyreport.google.com/eu-privacy/overview (accessed on 1. 12. 2017).

[134] This was at least the case in the first six months after the report form was launched. I. Kolar, *Smernice glede umika rezultatov iskanja po osebnem imenu*, Pravna praksa, 15/2015, p. 8 ff.

[135] See, for example, G. Dugar, *Pravica do pozabe na internetu*, in: A. Vlahek, M. Damjan (Eds.), Varstvo potrošnikov pri spletnem poslovanju, IUS Software, GV založba, Inštitut za primerjalno pravo pri Pravni fakulteti, Ljubljana, 2017, pp. 125-138, 247; P. Tepina, *Pozabljivi Google – prelomna sodba Sodišča EU o pravici do pozabe v razmerju do spletnih iskalnikov*, Pravna praksa, 21/2014, pp. 21-22; M. Brkan, *Odprta vprašanja prava varstva osebnih podatkov*, Pravna praksa, 31-32/2014, pp. 13-15; M. Prelesnik, *Novi izzivi informacijskega pooblaščenca*, Pravna praksa, 34/2014, p. 3; R. Lemut-Strle, *Pravica do pozabe – mit ali realnost*, Pravna praksa, 38/2014, pp. 13-15; P. Tepina, *Uresničevanje svobode izražanja in varstva zasebnosti skozi prizmo delovanja spletnih iskalnikov*, Pravna praksa, 20/2012, p. 10.

Article 29 Working Party in November 2015.[136] Some master's thesis in Slovenia have been defended on the topic as well.[137] The media has reported on the case and the substance of the »right to be forgotten« quite extensively.[138] Information on this right and useful guidelines on how to enforce it has been published also on the webpages of the national project *Safe on the Internet* (Sl. *Varni na spletu*).[139]

[136] I. Kolar, *Smernice glede umika rezultatov iskanja po osebnem imenu*, Pravna praksa, 15/2015, p. 8 ff.

[137] See, e.g. M. Kreča, *Pravica do pozabe*, Univerza v Ljubljani, Pravna fakulteta, 2017; Ž. Kotošek, *Primernost pravice do pozabe in njene izvedbe za varstvo zasebnosti*, Univerza v Mariboru, Pravna fakulteta, 2017.

[138] See, e.g., L. J. Kučić, *Pravica do elektronske pozabe*, Sobotna priloga, Delo, 7. 6. 2014; *Pomembna sodba: Evropejcem »pravica do pozabe«*, Mladina, 13. 5. 2014; V. Flegar, *Zaradi vašega članka ne dobim službe. Izbrišite ga!*, Dnevnik, 13. 3. 2017; MMC RTVSLO, *Nov mejnik na področju spletne varnosti: pravica do pozabe,* 2. 6. 2014; TV show on RTVSLO, *Pravica do pozabe*, 28. 5. 2014; S. Kisovec, *Pravica do pozabe*, Finance, 3.12. 2014; STA, *Varuhi osebnih podatkov: Prisotnih je še nekaj dilem, a pravica do pozabe učinkuje*, Dnevnik, 23. 9. 2014; STA, *Google zavrnil zahtevo Francije za pravico do pozabe tudi na neevropskih različicah*, Demokracija, 21. 7. 2015; etc.

[139] https://www.varninainternetu.si/2014/izbrisite-svoje-ime-in-priimek-iz-neprimernih-google-zadetkov/(accessed on 1. 12. 2017).

SPAIN

Rafael Allendesalazar
Juan José Montero

1. Internal Market and electronic commerce: Internet and e-commerce

1.1. Electronic Commerce, liability of Internet intermediaries

Question 1.1.1.

As in other jurisdictions, it is increasingly difficult to apply the principles in Directive 2000/31/EC in a more and more sophisticated environment. In particular, it is challenging to apply the liability exemption principle to players that interact with physical world services, such as collaborative economy platforms.

This is the case of online platforms that use complex algorithms to match supply and demand of services provided by third parties. A different degree of control is exercised by the platforms, that in some cases merely display potential service providers, in some cases filter them (by geographic area, price, etc.) without an active role in the review of the service provider, and in some cases take a more active role.

Question 1.1.2.

The test in L'Oreal v eBay was appropriate when adopted. However, as the digital ecosystem is growing in complexity and online platforms are growing in sophistication, reach and market power, the time to review the test might be approaching.

However, to increase the liability of intermediaries, it is necessary to have a good understanding of the services provided by the online platforms, the degree of control they have over the content/services they intermediate, and the technical capabilities they really have. As automatization plays a key role in the intermediation service (and the efficiencies are passed to final users), increasing

liability might require a control that reduces efficiency in the operation of the platform or just proves to be technically impossible.

Question 1.1.3.
Notice-and-take-down seems enough for most virtual services that merely affect the digital world and do not have implications for the physical safety of the user.

Question 1.1.4.
National legislation was adopted to protect intellectual property rights: Act 2/2011, of March 4, 2011 on Sustainable Economy, implemented by Royal Decree 1889/2011 of December 30, 2011 to govern the functioning of the Intellectual Property Commission (CPI). Such legislation defined the procedure before an administrative body, the CPI, to submit a notice –and-take –down order to an information society service provider.

If the information society service provider does not take down the infringing content, the intervention of electronic communications service providers (telecommunications operators) can be requested, after approval by a Court. This is allowed under article 11 of Act 34/2002 on information society services. Such an intervention can take the form of the suspension of the hosting service for services hosted in Spain, and even the form of web blocking for content hosted outside the European Union (and in another Member State).

Spanish Courts have not hesitated to adopt interim measures asking telecommunications operators to block access to web pages and mobile apps in order to make third party rights effective beyond intellectual propriety rights (unfair competition, terrorism, child porn, etc.). Such requests have been made even in relation with content hosted in another Member State of the EU. A good example is the interim measure adopted *inaudita parte* by Commercial Court no. 2 of Madrid against Uber on December 9, 2014.

Web (or app) blocking should not be the response to a potential infringement. Notice-ant-take-down and the suspension of the hosting service are more proportionate, particularly taking into account the risk of over-blocking (blocking access to legal content), the bypass to simple blocking measures (DNS filtering) and the high cost of more effective blocking measures. Only in case notice-and take-down and suspension of hosting are not effective, web blocking should be considered. In particular, interim measures ordering the blocking of webs and apps hosted in another Member State should be limited as contrary to the digital single market.

1.2. Consumer protection in relation to the internet and e-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.
In Spain, Direct Producers' liability was established in Act 1/2007 (Real Decreto legislativo 172007) and reinforced by amendments introduced by Act 3/2014. The concurrent liabilities of the seller, the importer, the producer, the insurer, etc. have generated difficulties and a growing case-law.

Question 1.2.2.
The full harmonization on contracts for the supply of digital content is a positive step for a genuine digital single market. The expansion of the basic rules on the sale of consumer goods to the supply of digital content is a positive approach.

Question 1.2.3.
Again, full harmonization is a positive step for a genuine digital single market.

Question 1.2.4.
The reinforcement of the harmonized EU consumer protection legislation in the digital single market is necessary despite obstacles and difficulties.

Question 1.2.5.
It is important to identify all the relevant legal relationships in a multisided market. The existing framework seems a solid base to rule the provision of intermediation services by online platforms. It might be necessary to make it effective, or even to complete it in order, for instance, to clarify the role of each entity in such a market, and the potential liabilities of the intermediary.

If the provider of the underlying service is a Merchant, again existing regulation seems to be enough to rule the relationship between service providers and final user (consumer). On the contrary, if the service provider is a non-professional service provider (peer to peer – P2P), the existing regulation on consumer protection does not apply. It does not seem reasonable to merely extend consumer protection legislation to these relationships. Initially, no unbalance exists between peers. Actually, non-professional service providers might require as much protection against users as users against non-professional service providers.

Question 1.2.6.
No landmark case has been decided in Spain in this area.

Question 1.2.7.
We understand that conflicts between service providers and online platforms will be increasingly common and one of the most relevant legal issues in the digital economy.

Businesses (many of them SMEs) dealing with online service providers such as online platforms (with global presence and in some cases billions of users) might find themselves under unbalanced situations. Complaints are increasingly common (Google case) and the European Commission has initiated actions to regulate such relationships Fairness in platform-to-business relationships).

However, the expansion of consumer protection legislation to these relationships does not seem to be the solution for the existing and potential conflicts. On the contrary, a stricter application of competition law and maybe some provision of unfair competition might be more effective.

Specific legislation will probably be necessary to protect the position of service providers. It seems early to define the guiding principles of such a legislation. Some kind of basic transparency obligations might probably apply across platforms. More specific obligations will probably have to be defined specifically for each type of platform.

As an example, service providers in the collaborative economy (drivers using Uber/Lift, bikers using Deliveroo, etc.) might require protection, which might be inspired by specific measures in labour legislation. However, the full application of labour law would ignore the commercial nature of this legal relationship as well as the economic rationale behind on-demand matchmakers as driver of substantial efficiencies for our societies.

1.3. Geo-blocking

Question 1.3.1
In May 2016, the European Commission published its proposal for a Regulation on geo-blocking and other forms of discrimination bases on customer's nationality, place of residence or place of establishment within the internal market.

The proposal prohibits geo-blocking and the rerouting of customers to a version of their online interface that is different from the online interface which the customer originally sought to access (Article 3). Furthermore, the proposal could impose the obligation for traders to sell passively, *i.e.* sales where the trader sales goods and those goods are not delivered cross-border to the Member State of the customer by trader or on his behalf (Articles 4 and 6).

There are doubts as to the effects the proposed regulation will have, once adopted, on rules governing contractual conflicts between the trader and the customers having their residence in other Member States and that have passively purchased the products.

With regards to the place of jurisdiction for European consumers, Article 18 of the (recast) Brussel I Regulation[1] provides that European consumer can always bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or, regardless of the domicile of the other party, in the courts of the place where the consumer is domiciled[2]. This provision applies if the other party is established in another Member State, if it has a branch, agency or other establishment in a Member States, or if, by any means, it directs its activities to that Member State (Article 17).

Furthermore, with regards to the law applicable to contractual obligations, Article 6 of the Rome I Regulation[3] provides that a contract concluded by a consumer with professional shall be governed by the law of the country where the consumer has his habitual residence, if that the professional: (a) pursues his commercial or professional activities in the country where the consumer has his habitual residence, or (b) by any means, directs such activities to that country or to several countries including that country, and the contract falls within the scope of such activities[4].

In this respect, recital 10 and Article 1 of the proposal for a Regulation on geo-blocking indicate that the mere fact that a trader carries out passive sales acts in accordance with the provisions of this Regulation should not be construed as implying that he directs his activities to the consumer's Member State. Furthermore, Article 1 of the proposed Regulation also provides that it shall not affect acts of Union law concerning judicial cooperation in civil matters, and that compliance with this proposal shall not be construed as implying that a trader directs his or her activities to the Member State where the consumer has the habitual residence or domicile within the meaning of the Brussels I and Rome I Regulations.

Notwithstanding these provisions, given the fact that the limits of what should be considered active or passive sales in the digital world are not always sufficiently clear, it has been argued that, merely by fulfilling its obligations on passive sales

[1] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. OJ L 351, 20.12.2012, p. 1–32.

[2] In Spain, a similar rule allowing the consumer to choose the jurisdiction is contained in Article 52.3 of the Civil Procedural Act (Ley 1/2000, de Enjuiciamiento Civil).

[3] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). OJ L 177, 4.7.2008, p. 6–16.

[4] In Spain, Article 67.1 of the Consumer Protection Act (Real Decreto Legislativo 1/2007, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias) expressly refers to Rome I to determine the applicable law. The Article concludes stating that, where the content of the applicable foreign law cannot be determined, alternatively Spanish law will apply.

under the proposed geo-blocking Regulation, a trader may find itself subject to the legislation and the jurisdiction of the Member States of its consumers, even if it had no intention of actively selling in those Member State. If this were to be the case, the obligation to sell passively could be particularly burdensome for SME traders.

Finally, it should be noted that, whereas these provisions on jurisdiction and on applicable legislation contained Rome I and Brussels I Regulations apply to "consumers", the proposed geo-blocking Regulation applies to "customers", a broader concept including consumers and businesses as end users. Thus, it could be argued that, on the basis of the geo-blocking Regulation, businesses acting as end users could also claim the benefit of Rome I and Brussels I.

1.4. Collaborative economy

Question 1.4.1.

Three are the most contentious issues in Spain: (i) the role of online platforms; (ii) tax issues; and (iii) labour law implications:

(i) The classification of platforms as service providers or mere intermediators: There are different administrative positions and court rulings on the role of collaborative economy platforms, in transport and accommodation. Some Courts decided that platforms are mere intermediaries. This was the case of Uber[5], BlablaCar[6] and Cabify[7] in transportation and Airbnb[8] in accommodation. Other courts have decided that the same platforms are service providers, particularly Uber[9]. Two important judgments are expected on the role of online platforms. A preliminary ruling by the Court of Justice of the European Union raised by the Commercial Court no 3 of Barcelona (C-424/15 Elite Taxi) and the extraordinary appeals raised to the Spanish Supreme Court against the already mentioned judgments of the Administrative Courts of Barcelona declaring Uber is only providing intermediation services.

(ii) The taxes imposed on peer-to-peer providers. It is often reminded that peers must be taxed when providing peer-to-peer services. A level playing field is necessary as professional service providers should not be disadvantaged against non-professional service providers. At the same

[5] Administrative Court of Barcelona no. 15 of Barcelona, judgments of 18 July 206 and 6 October 2016 and Administrative Court of Barcelona no. 17, judgment of 5 october 2016.

[6] Commercial Court no 2 of Madrid, judgment 2 February 2017.

[7] Commercial Court no 12 of Madrid, judgment 13 June 2017.

[8] Administrative Court no. 11 of Barcelona, Judgment of 29 November 2016.

[9] Provincial Court no 28 of Madrid, ruling of 23 January 2017.

time, as peer-to-peer services are substituting (at least partially) some services traditionally provided by professional service providers, it is important to guarantee that tax basis are not diminished by this new mode of industrial organization.

Spanish tax authorities have taken three relevant initiatives. Firstly, Spanish tax authorities made public a plan to supervise the fulfilment of tax obligations by entities contracting the provision of services though online platforms (*Plan General de Control Tributario 2017*) Secondly, a proposal was put for consultation for accommodation platforms to manage the payment of tourist taxes by non-professional service providers. No formal action has been taken after the consultation. Thirdly, Spanish tax authorities have confirmed that the sale of second-hand goods by non-professional sellers through online platforms is subject to the tax on property transfer and certified legal documents (4%) as well as income tax on the potential positive difference between the acquisition price and the selling price.

(iii) The legal nature of the relationship between service providers and online platforms. There is a discussion on whether such relationship is a labour law relationship or a mere commercial transaction between the service provider, which might be a self-employed person, and the platform providing an intermediation service for a fee charged to the self-employed person (or the person paying for the service provision). There was a very initial report from the labour authorities in Barcelona declaring the labour law nature of the non-professional drivers working with Uber in 2014/2015 (9 March 2015). The platform Deliveroo is having relevant conflicts with the individuals providing the delivery services. There is a growing consensus that some level of protection might be necessary for the individuals working with the platforms. Such protection, however, does not necessarily have to be based on the classification of such relationship as a labour law relationship. On the one hand, the key features of labour law in Spanish law, dependency and subordination, are not self-evident in the collaborative economy. Furthermore, such a classification might make many business models impossible due to the rigidity of Spanish labour law, particularly on-demand services. On the other hand, it is possible to increase the protection for the self-employed individuals by regulating the commercial relationship of intermediation, even with protective measures inspired on employment legislation.

Question 1.4.2.
Entry to the market by new competitors certainly increases consumers' choice and competition in the market. An example of the beneficial effects of the sharing economy is that after market entry in Spain by Uber in 2014, 2015 was the first year in decades that taxi rates were not increased in the city of Madrid.

The debate has focused on whether a level playing field exists and new comers compete with traditional service providers on equal terms. While traditional service providers enjoy privileges in terms, for instance, of licenses restricted in numbers, they also have obligations linked to such licenses. In some cases, obligations are particularly burdensome (public service obligations imposed on coach operators under concession rights), but in all cases, as professional service providers, traditional players are subject to the labour and tax obligations.

Newcomers, particularly peer-to-peer service providers, face restrictions to market entry in the form of licenses restricted in number and other restrictions linked to traditional market failures (rate regulation for taxis as to obstacle abuses and reduce transaction costs, etc.).

But newcomers are also free of many of the traditional restrictions imposed on traditional service providers. This has been the case particularly of peer-to-peer service providers, which in occasions have been considered to be outside of the scope of some restrictions. In parallel doubts about the application of some general provisions on tax law and social contributions have been automatically understood as exemptions benefiting such service providers.

Therefore, traditional service providers have initiated proceedings against online platforms for the breach of unfair competition law. Taxi associations and coach associations have been particularly active in filing complaints before commercial courts for unfair competition due to the breach of trade regulations, in particular the obligation to have a license. One of the complaints against Uber before the Commercial Court nº 3 of Barcelona resulted in the preliminary ruling to the Court of Justice of the European Union referred in Q1.4.1.

Question 1.4.3.
Three are the service providers under restricted market entry that have been affected by the collaborative economy: (i) local transport providers, including both taxy and Private Hire Vehicles (PHV); (ii) long distance road transport providers, that is coaches; and (iii) short-term rental services.

(i) The most contentious debate has been that on local transport. Taxi licenses are limited in number in all Spanish regions. In practice, the number of taxi licenses has been stable around 65,000 licenses over the last 35 years, despite growth in population and economic activity. Market entry is only possible through the acquisition of a license in the sec-

ondary market, which reached a price above EUR 200,000 in Madrid. The National Competition Authority has questioned this limitation, it has calculated that the elimination of such restrictions would reduce taxi prices around 10%, and has calculated the impact on the consumer welfare (see for instance the economic reports calculating the damage for final users in the cities of Malaga – 22 December 2015, and Cordoba – 15 January 2016).

PHV licenses were traditionally limited to a maximum of 1 for every 30 taxi licenses in a specific region. Such a restriction was abrogated in 2009 and reintroduced in November 2015. Regions refused to grant licenses despite the abrogation of the quantitative limitation in 2009. Only in November 2017 has the Supreme Court confirmed the right to be allocated a license in the interim period until 2015. As a consequence, between 10,000 and 15,000 licenses will be recognized over the next moths. Uber and Cabify are working with drivers that have this kind of license.

The National Competition Authority challenged before Courts the Decree reintroducing the 1:30 restriction in November 2015. Act 20/2013, of Guarantee of Unity of the Market, is the legal basis for this appeal. The 1:30 quantitative restriction is not the only restriction challenged. The Decree included other restrictions such as the obligation to have a fleet of a minimum of 7 vehicles, specific quality requirements for the vehicles (above those for taxis) and the prohibition to provide more than 20% of the services outside the region where the vehicle is registered. The judgment of the Supreme Court is expected for the beginning of 2018.

(ii) The debate on long distance coach service is more specific to Spain. Spain in one of the few countries in the EU where coaches have traditionally been more relevant that railway services in the provision of long distance passenger road services. The State and the regional authorities grant exclusive rights for the provision of services in specific routes. Internal cross-subsidies from high volume routes are used to fund low volume routes. This long-lasting model is under threat by collaborative economy models by BlaBlaCar or other local competitors. The national trade association of coach services challenged for unfair competition BlaBlaCar, as the platform would be providing transport services with no license. In first instance courts have upheld the position of BlaBlaCar.[10] It has been considered that BlaBlaCar provides no transport service,

[10] Commercial Court no 2 of Madrid, judgment 2 February 2017.

but merely intermediates connecting drivers and riders. Furthermore, it has been considered that drivers are not breaching the local transport legislation, as they are merely transporting closely connected passengers for a price that allows no benefit.

(iii) The debate on accommodation services has different angles. Firstly, regions have been introducing more restrictions for the provision of short-term rental services. For instance, the region of Madrid started to require a minimum stay of 5 nights. The National Competition Authority has been challenging these restriction before court based on the Act on Guarantee of Unity of the Market. Some restrictions have been declared null by Courts, such as the 5-night restriction in Madrid,[11] but also the prohibition of short-term rentals in in touristic areas in the Canary Islands.[12] Secondly, some cities, in particularly Barcelona, have declared a ban on new short-term rental properties, as well as hotels, in order to limit the growth of tourism in the city. Thirdly, in different regions, platforms have been fined for not checking the legality of the rentals making use of the platform. In Catalonia and Valencia, for instance, platforms were directly required to include in the listing of a property the license number granted by the authorities. As this obligation has not been met, different platforms have been fined by the regional authorities.

Question 1.4.4.

No major decisions have been adopted on this area. It seems clear that online platforms are providing professional services, at least as intermediation service providers. These services are clearly subject to consumer protection legislation when provided to consumers. A consumer protection association issued a report analysing the general trading condition in the contracts of the main online platforms (OCU (2016), Collaboration or Business? From value for users to a society with values).

The main challenge for consumer protection legislation is the provision of peer-to-peer services. Non-professional service providers will usually be outside of the scope of the consumer protection legislation. In this framework some protection might be necessary not only for the users of these services, but also for the service providers.

[11] High Court of Madrid, Administrative Chamber, section 8, judgment 31 May 2016.

[12] High Court of the Canary Islands, Administrative Chamber, section 2, judgment of 21 April 2017.

Question 1.4.5.
According to Spanish legislation, a trader is a physical or legal person, either private or a public administration, with a purpose related to its commercial activity, business activity, trade or profession (Royal Decree Act 1/2007, article 4). Case law requires continuity to consider a person as a trader.

Therefore, an individual which intermittently provides services or sells goods to other individuals is not considered a trader under the consumer protection legislation.

Question 1.4.6.
Legal rules can increase security in peer-to-.peer transactions within online platforms.

On the one hand, legal rules can increase transparency in rating and review systems. Such systems are heavily trusted by users, as academic literature has confirmed over the last years. However, academic literature has also confirmed that these systems are easily manipulated. Platforms have incentives to increase trust and security in the transactions, but at the same time, they have the incentive to grow the pools of service providers and users. Legal rules can increase transparency by forcing platforms to define the principles ruling the management of these systems: whether some ratings are eliminated and the reasons, what percentage is eliminated (as to make evident if negative comments are being deleted), etc.

On the other hand, other instruments to increase trust and security are: (i) the control of the identity of the parties in the platform (provision of some kind of ID); (ii) the control of minimum quality features of the service providers (driver's licenses for drivers and alike); (iii) the provision of insurance (at least secondary insurance); and (iv) management of payments for the parties.

These instruments are commonly used by online platforms to provide a safe contracting environment. However, these instruments might backfire as they might be considered as evidence of the fact that platforms are not merely intermediating but actually providing the underlying service.

Regulation could impose the provision of some of these features. Certainty could be given to all the users of the platforms, and to the platforms themselves, as to ensure that such a provision does not entail that the underlying service is the responsibility of the online platform.

In any case, authorities should refrain from overregulating. Platform rely on a delicate and dynamic equilibrium in the distribution of benefits and costs among all the players in the ecosystem. If the equilibrium is broken or merely ossified, the network effects on which rely platforms and which so much benefit users, might just disappear.

2. Digital media

Question 2.1.

When analysing the impact of the Judgement of the CJEU in *New Media Online*[13] on the concept of "programme" as applied in Spain, we should start from the outset by indicating that the definition of "programme" in Spanish Law is similar but not identical to that in Article 1(1)(b) of the Audiovisual Media Services Directive (AVMSD)[14].

The definition of "programme" in Spanish Law is contained in Article 2(6) of General Audiovisual Communications Act[15] (hereinafter, GACA), which defines separately television programs (subsection (a)) and radio programs (subsection (b)).

Television programs are defined as "a set of moving images, with or without sound, constituting an individual item within a schedule of a channel or a catalogue of programs. The following examples will be in any case considered as television programmes: feature-length films, sports events, situation comedies, documentaries, children's programmes and original drama, as well as live broadcastings of events, cultural or of any other type".

There are three main differences between the definitions of "programmes" contained in Article 2(6)(a) of GACA and in Article 1(1)(b) of the AVMSD.

The first difference refers to the inclusion in the list of examples of programs contained in the Spanish norm, of an explicit reference to the "live broadcastings of events, cultural or of any other type" that does not appear in the AVMSD. However, this additional example does not seem to materially enlarge the scope of the definition of "programme" contained in the AVMSD.

Two other differences relate to the concept of "catalogues" contained in Article 1(1)(b) of the AVMSD and in Article 2(6)(a) of GACA.

First, whereas as the AVMSD uses the term "catalogue", the GACA refers to "catalogues of programmes". This variance does not seem to have material implications, and in fact the reference to "programmes" included in the GACA when referring to catalogues appears to be redundant, since the provision is precisely defining what should be understood as "programmes".

The second difference with regards to the concept of "catalogues" is more noticeable: the GACA entirely omits the fact that catalogues are considered as

[13] Judgment of the Court of 21 October 2015, *New Media Online GmbH v Bundeskommunikationssenat and Der Bundeskanzler*, Case C-347/14, (ECLI:EU:C:2015:709).

[14] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive); OJ L 95, 15.4.2010, p. 1–24.

[15] Act 7/2010 on General Audiovisual Communications, of March 31st. BOE nº 79, 1.4.2010.

programmes when they have been "established by a media service provider and the form and content of which are comparable to the form and content of television broadcasting". This could be referred to as the comparability criterion defined in Article 1(1)(b) of the AVMSD.

This omission of the comparability criterion in the GACA could become particularly relevant in the light of importance given by the CJEU to that criterion in paragraphs 18 and 19 of its Judgement in *New Media Online*. In that case, the CJEU concluded that giving access to a mass audience, through the subdomain of a website of an online newspaper, to a catalogue of more than 300 videos of short duration consisting of local news bulletins, sports and entertainment clips, was included in the concept of "programme" within the meaning of Article 1(1)(b) AVMSD, relying essentially on the fact that that catalogue of videos *"can be compared to the form and content of television broadcasting"*.

The fact that the GACA does not mention this comparability criterion has led some authors to indicate that the notion of programme could be more limited under that Spanish norm than under the AVMSD[16].

But we are not aware of any case where the absence of that criterion in the GACA would have led, in practice, to applying a narrower notion of programme. What's more, in a recent decision[17] the Spanish media regulator (CNMC[18]) has expressly referred to the Judgement of the CJEU in *New Media Online* in a case where it imposed a fine on the Spanish National Professional Football League (LNFP) after concluding that it had infringed the GACA by denying access to a television organisation to the football fields to prepare short news reports. Based on that Judgement of the CJEU, the CNMC argued that, by offering on its website access to short videos with résumés and interviews, each video should be considered as a programme, and the LNFP was thus acting as an audiovisual media services provider, and was therefore subject to the obligations imposed on such providers but the GACA.

We can thus conclude that the definition of "programme" in the GACA does not entirely coincide with the one contained in the AVMSD. The main difference is that the notion of "catalogues" contained in Article 2(6)(a) of GACA does not mention the comparability criterion included in Article 1(1)(b) of the AVMSD, the importance of which has been highlighted by the CJEU in its *New Media Online* Judgement. However, in practice this difference in the wording of those

[16] DE MIGUEL ASENSIO, P.A. *Caracterización de ciertos sitios de internet como servicios de comunicación autiovisual*. La Ley Unión Europea. Number 31 – December 2015. pp. 1-8.

[17] Decision of the CNMC of June 1st 2017 in case SNC/DTSA/020/17/LNFP.

[18] Since October 2013, the main Spanish sector regulators were merged with the competition authority to form a single entity, the Comisión Nacional de los Mercados y la Compentencia (CNMC), with two chambers, one for sector regulations, including media, and another one for competition matters.

provisions does not seem to have resulted in material differences in the way the concept of "programme" is being applied in Spain. In particular, the Spanish media regulator has expressly relied on the interpretation of the "programme" made by the CJEU in *New Media Online* when applying the GACA. Furthermore, in the event such discrepancies between the wording of Article 2(6)(a) of GACA and Article 1(1)(b) of the AVMSD were to be raised before a Spanish court, we believe that court would have no difficulty in applying the well-established principles of primacy and interpretation in conformity with Community Law to overcome any differences in the wordings and to interpret the notion of "programme" in the context of the GACA in line with the AVMSD, as applied by the CJEU in *New Media Online*.

Question 2.2.

The current AVMSD does not apply to user-generated content (UGC) platforms[19], since the provider of the video-sharing platform usually does not have an editorial responsibility for the content stores in the platform.

However, there is an increasing convergence and competition between these services and other traditional audio-visual media services. In this respect, it is worth noting that recital 24 of the AVSMD already recognized the need to interpret its scope dynamically, to take into account developments in television broadcasting so as to include *"on-demand audiovisual media services that [...] are 'television-like', i.e. that [...] compete for the same audience as television broadcasts, and the nature and the means of access to the service would lead the user reasonably to expect regulatory protection within the scope of this Directive"*, and *"prevent disparities as regards free movement and competition"*.

Therefore, we believe the proposal to amend the AVMSD and to include new players offering audiovisual content via the internet, and particularly video-sharing UGC platforms, is a step in the right direction, as it levels to a certain extent the competitive playing field between these two types of audio-visual media services providers. This alignment is particularly important with regards rules to protect minors and to combat hate-speech, as young people, who would be particularly vulnerable, increasingly view audio-visual content form UGC platforms and not from traditional providers.

Alignment with respect to other AVMSD rules such as product placement, sponsoring, advertising may seem more difficult to impose other rules since UGC platforms usually do not have an editorial responsibility for the content stored in the platform.

[19] These platforms are often also referred to as user-created content (UCC) platforms.

The Spanish legislation does not currently contain specific rules for UGC platforms. However the CNMC has recently declared that the rules on advertisement of alcoholic beverages applicable to traditional television broadcasting should also apply to platforms that allow viewing programs from mobile devices[20]. The CNMC argued that excluding such platforms would be *"illogical"* given the fact that mobile devices are increasingly used to watch television programs, particularly by young people.

Question 2.3.

We are not aware of any specific conflict related to the Spanish media regulator (CNMC) attempting to apply national rules on audio-visual media service providers established in other Member States.

There is however an interesting case reflecting the reverse problem: the Latvian media regulator filed a complaint before the CNMC against FOX NETWORK GROUP ESPAÑA, SLU (FNG), a Spanish subsidiary of the FOX NETWORK GROUP that acts as editor of the FOX CHANEL broadcasted in Latvia. The Latvian media regulator considered that one of the chapters of *Walking Dead*, broadcasted during the hours of protection established under the Latvian audiovisual legislation, contained scenes of physical violence, blood and terror, thus violating the said Latvian legislation. The CNMC finally dismissed the complaint as it concluded that FNG had not violated the restrictions imposed by Spanish audiovisual legislation on on-demand television providers –that differ and are more lenient that those imposed on open-air television broadcasters– to protect minors from programmes containing violence[21].

Question 2.4.

There is a broad consensus in favour of requiring that media regulators should be independent. This is clearly reflected in the ERGA Report on the independence of NRA:[22] *"there seems to be a large shared opinion among ERGA members that NRAs should be established as entirely independent entities, legally and functionally autonomous from other institutional bodies and from all organisations related to the provision and distribution of audiovisual media services, to ensure that NRAs act impartially from any political, national body or any market player. The new EU Directive should include a specific provision highlighting this."*

Independence ensures that regulators can make decisions free from the influence both of elected officials and private parties, including the regulated entities.

[20] Decision of the CNMC of May 9th 2017 in case CNC/DTSA/266/17/ – AUTOCONTROL BEBIDAS ALCOHÓLICAS.

[21] Decision of the CNMC of June 1th 2017 in case IFPA/DTSA/001/17/ -FOX LETONIA.

[22] ERGA Report on the independence of NRAs. ERGA (2015)11

The ERA has explained why independence, is important specifically for media regulators: *"the independence of regulatory bodies in the communications sectors is key to their effectiveness, supporting the fulfilment of their role to protect the interests of citizens and consumers and, at the same time, to ensure a predictable and dynamic competitive environment in their sectors. At a high level, regulators should be able to carry out their regulatory tasks without direction or interference from political or commercial interests. In the audiovisual field, in particular, the principle of independence is central to enable regulators to have effective oversight of the sector and to carry out their regulatory functions efficiently in areas covered by the European audiovisual framework such as audience protection, including the protection of minors, freedom of expression, diversity, pluralism and other areas such as media ownership."*[23]

On top of those reasons, we believe ensuring the independence of media regulators is particularly important given the fact that in many European countries, including Spain, publicly owned audiovisual content providers compete with private media companies. Only media regulators that have sufficient financial, operational and decision-making independence will be in a position to ensure that elected officials do not unduly favour public media providers in the detriment their private competitors, and that any difference in the regulation applicable to these two categories of content providers is strictly justified and proportional to the public policy goals specifically imposed on the publicly owned audiovisual content providers.

Independence of regulators should not be considered as a given, and should be enshrined in the basic European legislation applicable to each sector. Spain provides an excellent practical example of the advantages of explicitly protecting the independence requirement in the legislation.

In 2012, the newly elected Spanish Government decided to merge several sector regulators together with the national competition authority into a new single unified authority, the CNMC. It also decided to remove all the members of the board of the previous authorities before the expiry of their terms of office, and to appoint new members of the board of the CNMC. The members of the former Competition Authority could not legally challenge their dismissal, as Regulation 1/2003 surprisingly does not explicitly require that national competition authorities are independent. By contrast, two members of the Telecoms regulator were able to appeal their dismissal on the basis that it was contrary to the provisions ensuring the independence of the national regulators contained in Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services. And finally, the CJEU indeed confirmed that the rules contained in that Directive preclude *"the dismissal of the President and*

[23] ERGA statement on the independence of NRAs in the audiovisual sector. ERGA (2014)03.

a board member, of the collegiate body running the merged national regulatory authority, before the expiry of their terms of office, in the absence of any rules guaranteeing that such dismissals do not jeopardise the independence and impartiality of such members."[24] See more on this case in Q3.4.

This example clearly illustrates the importance of explicitly proclaiming in the European Legislation the independence of the national regulators, and also of specifying the requirements of competence, independence, impartiality and transparency needed to ensure that independence. We thus conclude that the introduction of such independence requirements for media regulators at EU level should be warmly welcomed.

3. Digital infrastructures

Question 3.1.
Spain did not have rules on net neutrality before the adoption of regulation (EU) 2015/2120.

Operators active in Spain have launched zero-rating offers and no reaction from the competent authority (the Ministry, not the National Regulatory Authority) has taken place.

Question 3.2.
Migration from analogue to digital technology has created divergence in the European telecommunications. Traditional analogue services such as public telephony and leased lines were technically harmonized at a global level. IP services, on the contrary, present a lower level of technical harmonization. Networks in the Member States are increasingly divergent: different degrees of fibre deployment, different architectures (fibre to the cabinet, fibre to the home, etc.) different technical solutions, etc. At an EU level, little action has been taken to harmonize the market. Proposals by the Commission to impose harmonized access products were not successful. This is an obstacle to provide EU wide services, particularly in the business segment.

As regards broadband, the situation in Spain is quite exceptional, as three parallel fibre networks are under development and all of them are very ambitious in terms of deployment (more than 10M households). Different reasons explain this situation: the strategy of the operators, in particularly the market leader Telefónica, geographical reasons (the concentration of the population in very dense cities and towns makes the deployment cheaper), but certainly regulation has played an important role. The Spanish NRA refused to up-date the

[24] Judgment of the Court of 19 October 2016, *Xabier Ormaetxea and Bernardo Lorenzo v Administración del Estado* Case C-424/15. ECLI:EU:C:2016:780.

access regulation regarding fibre networks. In January 2009 CNMC decided to exclude access to fibre from the *ex ante* regulatory obligations imposed on Telefónica, as such an obligation was excluded for bandwidths above 30Mbps. It was only seven years later, in February 2016, that CNMC finally updated the *ex ante* access obligations and then, direct access to fibre was excluded in all the major cities in the country, as competition already existed in those geographic areas. In practice, CNMC granted a 7 year "regulatory holiday" to Telefónica, and the obligation in EU Directive and Spanish legislation to review telecom markets every 3 three years was breached. In 2009 Telefónica started to execute an ambitious strategy to deploy fibre, and to bundle the provision of fibre based services (fixed telephony, broadband access to the internet and audio-visual services) to mobile services. Alternative operators such as Orange and Vodafone had to deploy their own fibre networks (and acquire smaller competitors with some deployment) to protect their investment in mobile networks.

By 2017, Spain presents one of the highest penetration rates of FTTH in the EU, as well as three competing networks.

Question 3.3.

Spain traditional had a very high rate of spectrum dependent Digital Terrestrial Television against other technologies more popular in other countries (satellite, cable, IPTV). Therefore, spectrum policies to favour mobile services against DTT services has created more conflicts in the past. As fibre deployment of contributing to the reduction of DTT relevance, spectrum redistribution might become less of an issue in the future.

Question 3.4.

In 2013 a cross-sectorial NRA, the CNMC, was created. It assumed the powers of the previously existing National Competition Authority and the National Regulatory Authorities with sector specific competences in telecommunications, audio-visual, postal services, energy, railways and airports.

A conflict arose as the President of the telecommunications NRA, the CMT, as well as one of the members of the board, challenged the national Decree which ended their term of office, as contrary to the independence requirement in Directive 2002/21/EC (Framework Directive).

A request for a preliminary ruling was raised by the Spanish Supreme Court to the Court of Justice of the European Union. On 19 October 2016 the CJEU decided that "Directive 2002/21/EC [...] is to be interpreted as not precluding, in principle, national legislation which entails the merger of a national regulatory authority [...] with other national regulatory authorities". However, the CJEU decided that Article 3(3a) of the Framework Directive "is to be interpreted as

precluding – on the sole ground that an institutional reform has taken place involving the merger of a national regulatory [...] the dismissal of the President and a board member, members of the collegiate body running the merged national regulatory authority, before the expiry of their terms of office, in the absence of any rules guaranteeing that such dismissals do not jeopardise the independence and impartiality of such members."

The conflict has been finally solved as both the former President and member of the board of CMT have been appointed as members of the board of CNMC in the regular renewal of members of the board that took place in 2017.

The concentration of powers in a single authority has created further issues. On the one hand, competences traditionally granted to the sector specific authority were now given to the Ministries. This is the case of licenses, notifications and numbering, as well as new powers such as the control of net neutrality rules. The same strategy was followed on other competences in energy, postal services, etc. The reason behind such a decision was to reduce the concentration of powers in a single independent authority. However, doubts have been raised on competences that Directives require to be handled to independent authorities might have been granted to the Government, particularly in the energy industry.

On the other hand, the internal functioning of such a complex institution has also raised doubts. Two chambers were created to decide on competition law issues, on the one side, and regulatory issues, on the other side. The concentration of competition law and sector specific regulation was supposed to avoid contradictions in the application of both sets of rules to the same cases. Conflicts are still possible, but they are decided through the intense exchange of reports among the services of the competition directorate and the relevant sector specific directorate. In the same vein, the most relevant cases are decided in a joint meeting of both the competition and the regulatory chambers (10 members) with the president of the CNMC, who also chairs the competition chamber, deciding in case of tie in votes. Doubts have also been raised on the ability of the 5 members of the regulatory chamber to actively supervise the intervention in industries as complex as telecommunications, energy, transport, and posts.

A political agreement has been reached to reform CNMC and to divide it in two different authorities, one for competition law and another for sector specific regulation.

4. Data in the digital economy

Question 4.1.

A bill prepared by Government to be voted in Parliament was made public in mid-2017.

Question 4.2.
Large, businesses are working to meet the very demanding requirements in GDPR and the national legislation. It has been common to set-up specific working groups and to appoint specific individuals to lead such an effort, increasing the seniority of such individuals to reinforce their position in the company. Smaller businesses are lagging behind in such an effort.

Question 4.3.
There has been limited activity on this from in Spain. There is no legislative activity and very limited opinions / guidelines from the Spanish Data Protection Authority.

The Action Plan of the Spanish DPA for 2015-2019 states generically that studies will be made between 2016 and 2019 on big data, IoT, smart cities, smart cars, smart home, mobile apps, drones and other technologies.

So far, A Code of Good Practices on Big Data was published in 2017. No other study / report / opinion has been published.

The Spanish Data Protection Agency was particularly active in the past on cloud computing. Two guidelines were published in 2013 (both for service providers and customers).

Smart meters, particularly in the energy industry, seems to be of particular interest for the Spanish DPA.

Question 4.4.
Following the Google Spain case, there have been some decisions of the Spanish Data Protection Authority on the so-called "right to be forgotten". Some principles can be extracted from these decisions.

Firstly, the Spanish DPA has confirmed that the request must be filed before the right corporation of the group. It is often the case that large multinationals have local corporations providing support to the group, but such corporations do not provide services to the public. This is the case of Google, Microsoft, or Yahoo. The DPA has usually supported the argument of the search engines and requests must be submitted through the specific forms to the relevant corporation.

Secondly, requests "to be forgotten" can be submitted not only to the corporation providing search services (i.e. Google) but also to the entity that published the relevant information with personal data, (i.e. a newspaper). In this case, it is of relevance to distinguish between the elimination of the information in the newspaper itself, and the elimination of the technical signals used by the newspaper to automatically communicate with the search engines. The Spanish DPA supports requests to eliminate the relevant signals, so that the information is not displayed by search engines, rather than requiring the elimination of the informa-

tion in the original source (Decision of 4.10.2016 Periodico de Catalunya). This position has also been supported by the Supreme Court (Judgment of 15.10.2015).

Thirdly, there have been cases where the DPA has questioned the decision of the search engine on whether the information is relevant or not. The DPA has not provided very specific guidelines on how to balance the "right to be forgotten" with the right to information and expression. However, it has been clear in the indication that it is the obligation of the search engine to justify its decision not to delist an information based on its relevance (Decision 11.5.2015). Furthermore, the balance has to be made not on the relevance of the information when it was published or linked, but at the present. For instance, the Spanish DPA has considered that an information about how a professional provided a service is not relevant when the individual ceases to provide the professional service (Decision 24.11.2014).

Fourthly, the Spanish DPA considered that in case search engines desire to include some kind of message when retiring links or content, such message should not appear as linked to specific requests for search where for instance the name of a person is included, but rather as a general message not related to specific searches (Decision 9.9.2016 Google).

SWEDEN

Olivier Linden*

Introduction

In a wide range of areas, from broadband penetration to the rate of digital literacy or the proportion of consumers buying goods or services online, Sweden features in the top tier of EU countries.[1] Stockholm, the country's capital, is home to a dynamic eco-system for start-ups which ranks second among European cities.[2] With a developed export-oriented economy and a high level of digitalization, Sweden has embraced the European Commission's objective to achieve a Digital Single Market (DSM).[3] Together with other like-minded countries, Sweden is even pushing for more ambitious initiatives at EU level, for instance within the framework of the Digital-9 Group.[4]

Yet, in spite of its interest in achieving a DSM, Sweden is sometimes at odds with the line adopted by the majority of EU States and by the EU institutions. This is for instance the case with regards to the level of market intervention where Sweden has a more liberal approach than many of its partners in e.g. regulating online platforms. Similarly, Sweden has traditionally put a stronger emphasis on the freedom of speech when balancing it with other interests such as data

* Swedish National Board of Trade (Kommerskollegium). With valuable contribution from Philip Levin.

[1] European Commission "Europe's Digital Progress Report" SWD(2017) 160 (27 April 2017).

[2] See for instance, European Digital City Index 2016 (www.digitalcityindex.eu). See also Alana Semuels "Why Does Sweden Have So Many Start-Ups?" The Atlantic (28 September 2017) and James Temperton "Europe's hottest startups 2016: Stockholm" wired.co.uk (16 September 2016).

[3] European Commission "A Digital Single Market Strategy for Europe" COM(2015) 192 final.

[4] See Government press release "Ann Linde takes initiative at EU level for a 'Digital 9' group" (5 September 2016).

protection. More recently, Sweden has voiced its opposition to the proposal to introduce a European digital tax.[5]

It is in this context of European integration and of the digitalization of the economy that the Swedish regulatory framework is to be understood. In this report, we review the Swedish rules applying to e-commerce (Section 1), digital media (Section 2), digital infrastructure (Section 3) and data in the digital economy (Section 4). The report is intended to serve as a basis for the general report on the "Internal Market and the Digital Economy" to be presented at FIDE's 2018 Congress. It addresses the questions prepared by the General rapporteur in the order they are presented in the questionnaire.

1. Internet and e-commerce

1.1. Liability of Online Intermediaries

The concept of liability of online intermediaries covers a wide range of situations.[6] As a result, an overview of the Swedish rules on the liability of online intermediaries calls for a review of a variety of laws on e.g. intellectual property, e-commerce, data protection as well as the protection of fundamental rights such as the freedom of speech, the right to privacy or the freedom of the press. Below is a short introduction to the most relevant laws.

First, the Act on Bulletin Board System (the "*BBS Act*")[7] imposes an obligation on certain online intermediaries to supervise their services and to remove messages with obviously unlawful content. The BBS Act applies only to those intermediaries which provide or operate websites where users can post and read messages.[8] The BBS Act covers messages which incite to riots or to racial hatred or contain child pornography or unlawful depiction of violence as well as infringements of copyrights and related rights.

Second, the exemption of liability set in the E-Commerce Directive (2000/31/EC) is regulated in the Swedish E-Commerce Act.[9] In that respect, the exemp-

[5] See for instance Politico "Bitter divisions undermine Europe's digital tax plans" (29 September 2017).

[6] It applies to various types of online intermediaries, from access providers to online market places, social networks, media platforms or search engines. The control exercised over user-generated content vary between intermediaries and, as a result, so does their liability with regards to such content. Further, user-generated content may raise a variety of compliance issues, from intellectual property infringements to violations of privacy, defamation or criminal activities. Each issue is subject to an own sets of rules on e.g. establishing an infringement, accountability as well as remedies and sanctions.

[7] Act on Responsibility for Electronic Bulletin Boards (1998:112) (*Lag om ansvar för elektroniska anslagstavlor*).

[8] Note that the BBS Act does not apply to operators which are protected under the rules on freedom of speech, i.e. mass media companies and persons who have obtained a so-called "publishing certificate". The protection of holders of "publishing certificates" is discussed below in Section 4.2.

[9] Act on Electronic Commerce (2002:562) (*Lag om elektronisk handel och andra informationssamhällets tjänster*).

tion of liability for mere conduit (Section 16 of the E-Commerce Act), caching (Section 17) and hosting services (Section 18) mirrors the rules set in Articles 12 to 14 of the Directive.

Third, the EU rules on injunctions set in the Infosoc-Directive (2001/29/EC) and the Enforcement Directive (2004/48/EC) are transposed in various intellectual property legislations. In particular, a new Section 53b was introduced in the Copyright Act[10] in order to implement Article 8(3) of the Infosoc-Directive. For intellectual property rights, other than copyrights, the provisions on injunction against intermediaries set in Articles 9(1)(a) and 11 of the Enforcement Directive were implemented in Sweden by way of amendments to the relevant IP-laws.[11]

Finally, other rules may apply such as those set in the Personal Data Act[12] with respect to the obligations of data controllers[13] or the Swedish consumer rules with regards to unfair marketing practices by the users of online intermediaries.[14]

Question 1.1.1.
Specific definition problems of the concept of online intermediaries have arisen with respect to (i) the scope of the BBS Act and (ii) the injunction mechanism in copyright cases.

(i) Online intermediaries under the BBS Act
The BBS Act has been criticized in the doctrine for its lack of clarity, notably with respect to its scope of application. It applies to "Bulletin Board Systems" (*Elektroniska anslagstavlor*) which several authors found a difficult concept to interpret. Some have argued that the concept of interactive websites would have been more appropriate.[15] Others have called for broadening the scope of application of the

[10] Copyright Act (1960:729) (*Lag om upphovsrätt till litterära och konstnärliga verk*).
[11] See respectively: Chapter 8, Section 3 in the Trade Marks Act (2010:1877) (formerly, Section 37b in the Trade Marks Act (1960:644)), Section 57b in the Patents Act (1967:837), Section 35b in the Design Protection Act (1970:485), Section 15 in the Trade Names Act (1974:156), Section 9b of the Act on the Protection of Topographies for Semiconductor Products (1992:1685), and Chapter 9, Section 2 of the Act on the Protection of Plant Breeders' Rights (1997:306).
[12] Personal Data Act (1998:204) (*Personuppgiftslagen*).
[13] In order to avoid repetitions, the rules on data privacy are discussed in Section 4 of this report.
[14] Section 23 of the Swedish Marketing Act (2008:486) (*Marknadsföringslagen*) prohibits unfair marketing and extends that prohibition to those who significantly contribute to such marketing. The Swedish courts have stated that this prohibition applies to newspapers which publish ads which are manifestly unfair (Market Court (*Mardnadsdomstolen*) in case 1995:2). To the best of our knowledge there is no specific case-law on online intermediaries but we understand that the Swedish Consumer Agency (*Konsumentverket*) has discussed this issue with social media providers.
[15] Forsman "*Internetpublicering och sociala medier, en juridisk vägledning*", 4 uppl. 2011 (p.58).

BBS Act to the provision of electronic storage capacity, which would include hosting companies and providers of banner advertising.[16]

A recent Government-commissioned report noted that, almost 20 years after its entry into force, there were almost no judgments interpreting the BBS Act.[17] In the absence of case-law, it is therefore difficult to assess whether the criticised concept of "Bulletin Board Systems" is too narrow or outdated.

(ii) Online intermediaries under the Copyright Act

Until recently, the Swedish and EU rules on injunctions in intellectual property rights differed from each other. On the one hand, the Infosoc-Directive grants a possibility to issue an injunction against access providers whose services are used to commit copyright infringements, regardless of their relationships to the third-party infringers.[18] The Swedish legislator, on the other hand, restricted this remedy to those access providers which had actively contributed to such infringement.

According to Section 53b of the Copyright Act, a court may issue an injunction prohibiting, on penalty of a fine, a party that commits, "*or contributes to*", an act constituting an infringement of copyrights.[19] At the time of implementation of the Infosoc-Directive (2005), the Swedish preparatory works clarified that the verb "contribute" (Sw. *medverka*) was to be understood in the criminal law sense.[20]

Thus, intermediaries such as Internet Service Providers (ISPs) having a mere passive role in the infringement were not meant to be caught by the Copyright Act. Instead, the preparatory works noted that "*something more than the mere provision of internet access*" was required for Section 53b to apply. The preparatory works did not define this requirement but, as an example, stated that intermediary liability would be triggered if there were a contractual link between the intermediary and the copyright infringer and the intermediary was aware of an on-going infringement.[21]

[16] Carlén-Wendels "*Nätjuridik, Lag och rätt på internet*", 3 uppl. 2000 (p.70).

[17] See Government-commissioned report (2016:7) "*Integritet och straffskydd*" (February 2016), Chapter 16 which provides an overview of the critics of the scope of application of the BBS Act.

[18] See case C-314/12 *UPC Telekabel* at para. 32 and 35.

[19] Note that, originally, the draft bill on the implementation of the Infosoc-Directive did not include any explicit provision on intermediary liability. Instead, the Swedish Government found that existing provisions on injunctions against infringers were sufficient to fulfil the obligations set in Article 8(3) of the Directive. The Swedish Council on Legislation (*Lagrådet*, an advisory body on new legislation) objected to this interpretation and as a result, the Government introduced this new formulation in its bill.

[20] Government Bill 2004/05:110 (p. 339-340).

[21] Subsequent preparatory works discussed the extension of the scope of intermediary to include all ISPs but none resulted in a proposal to amend Section 53b of the Copyright Act. See Ministry of Justice

Compliance of these rules with the Infosoc-Directive was tested in a recent case opposing film and music producers to a Swedish ISP (B2 Bredband). The claimants had petitioned the Patent and Market Court (*Patent- och marknadsdomstolen*) to issue an injunction ordering B2 Bredband to block its users' access to websites that were providing films and music in violation of the Copyright Act.

In its 2015 ruling,[22] the Patent and Market Court acknowledged that the websites in question (The Pirate Bay and Swefilm) were making available protected works and that users of B2 Bredband might have access to them. However, the Court found that B2 Bredband had not contributed "in a criminal law sense" to the copyright infringement and rejected the claimants' petition.[23]

This ruling was overturned by the Patent and Market Court of Appeal (*Patent- och marknadsöverdomstolen*) in its judgement of 13 February 2017.[24] The Court of Appeal found that it was possible to issue an injunction against an intermediary whose services are used to commit a copyright infringement, even if the intermediary only provides internet access to its customers. The Court of Appeal rejected the view developed in the preparatory work that some kind of special relationship must be established between the intermediary and the third-party infringer. Instead, the Court of Appeal referred to the *UPC Telekabel*-case,[25] to interpret the Copyright Act in conformity with the Infosoc-Directive.

The Patent and Market Court of Appeal ordered B2 Bredband, on penalty of fine, to block access to the websites of The Pirate Bay and Swefilm for a period of three years. This judgment is final and cannot be appealed. At the time of writing, it remains unclear if the Copyright Act will be formally amended in order to reflect this ruling.

Memorandum on the implementation of the Enforcement Directive (Ds 2007:19, p. 223-224), Ministry of Justice Memorandum "*Musik och film på internet*" (Ds 2007:29, p. 356) and Government Bill (2008/09:67) on the implementation of the Enforcement Directive, p. 195.

[22] Patent and Market Court in case T-15142 *Universal Music Aktiebolag, Sony Music Entertainment Sweden AB, Warner Music Sweden Aktiebolag, Nordisk Film A/S, Aktiebolaget Svensk Filmindustri v. B2 Bredband AB* (27 November 2015).

[23] The Court based its reasoning on the preparatory works of the Copyright Act and argued that this law was in line with the Infosoc-Directive. It noted in particular that the Directive gave the Member States a broad discretion in implementing the rules on intermediary liability and merely provided for a possibility, rather than an obligation, to issue an injunction against intermediaries.

[24] Patent and Market Court of Appeal in case PMT 11706-15 *Universal Music Aktiebolag, Sony Music Entertainment Sweden AB, Warner Music Sweden Aktiebolag, Nordisk Film A/S, Aktiebolaget Svensk Filmindustri v. B2 Bredband AB* (13 February 2017).

[25] Case C-314/12 *UPC Telekabel*.

Question 1.1.2.

To the best of our knowledge, the *L'Oréal* judgment[26] has not led to any practical issues in Swedish law. In particular, the test put forward by the CJEU has not been questioned by Swedish courts.[27]

Although reasonable in our view, the concept of "active role" set in that ruling may raise some practical difficulties of interpretation. The variety of services provided by online intermediaries and the differences in their business and technical models can make it difficult to foresee for every situations when sufficient control is exerted over user-generated content to trigger liability. For online platforms, it may be especially challenging to assess how new control requirements imposed by the EU legislator within the scope of the DSM Strategy may affect their liability under the E-Commerce Directive.[28]

There is a risk that the liability exemption regime loses its strength and that this in turn negatively affects important interests such as innovation and growth which the Directive intended to promote. Without denying the rise of serious concerns since the adoption of the Directive (from hate speech to privacy concerns and IP-right infringements), it is in our view important to maintain a holistic approach on growth and innovation when discussing individual measures on e.g. data protection, illegal content or video-sharing platforms.

Question 1.1.3.

The E-Commerce Act does not contain any notice-and-take down mechanism. At the time of implementation of the E-Commerce Directive, the Government found that this was neither required under EU law nor practical.[29] It also noted that such mechanism was already partly in place under the BBS Act with regards to messages which are obviously in breach of public order[30] or of copyrights and related rights.

[26] Case C-324/09 *L'Oréal v. eBay*.

[27] The concept of "active role" in the *L'Oréal* case was for instance mentioned in a copyright infringement judgment by the Stockholm District Court (*Tingsrätten*) without being challenged (case T-10848-09 (27 June 2013)).

[28] Interestingly, we note that the European Commission states that proactive measures recommended in its recent guidelines on tackling illegal content online "*do not in and of themselves lead to a loss of the liability exemption*." (COM(2017) 555, p.13).

[29] Government Bill (2001/02:150) on the implementation of the E-Commerce Directive, p.98-99. Note that save with respect to video-sharing platforms, there is no current EU proposal setting up a compulsory notice and take down mechanism (see COM(2016) 287 final with regards to video-sharing platforms and COM(2017) 555 final for the Commission's guidelines on "Tackling Illegal Content Online").

[30] Specifically messages which incite to riots or to racial hatred or contain child pornography or unlawful depiction of violence.

As illustrated with the recent ruling of the ECtHR in the *Pihl v. Sweden* case,[31] the BBS Act is limited in scope and does not cover defamation or breach of privacy. In 2016, a Government-commissioned report proposed to include unlawful threats and unlawful violations of privacy within the scope of the BBS Act.[32]

Several factors motivated this proposal. Notably, the report noted that since 1998, when the BBS Act was adopted, new services had appeared and, as a result, the damages posed by unlawful threats and violation of privacy had become more severe. The increased use of tools for sharing and endorsing ("liking") messages with unlawful content made the problem more acute. At the same time, it became increasingly difficult to identify the authors of such messages which can post anonymously. It is not either always feasible or appropriate to initiate proceedings against all persons who have shared or liked messages with unlawful content. It is, in that respect more effective to target at the intermediary who is in charge of the website where those messages are posted. The report also noted that, in many cases, the authors of unlawful messages have no possibility to delete them and that website operators are therefore more suited to delete or block those messages.

The report did not however propose to extend the notice-and-take down mechanism to other crimes, such as defamation. Defamation, the report noted, is difficult to assess as it calls for a complex review of a person's reputation which takes into account such factors as the person's position in society or a given group. It is therefore seldom possible for an online intermediary to find that a message is "obviously" defamatory.

At the time of writing, it is unclear if and when the proposals put forward in this Government-commissioned report will result in an amendment of the BBS Act. Our understanding is that the Government is working on a bill which would at least discuss some of the proposals made in this report.

Question 1.1.4.

To the best of our knowledge there are no major difficulties with respect to injunctions, other than those mentioned under Q 1.1.1 above.[33] As noted, in the *B2 Bredband* case,[34] the Swedish Patent and Market Court of Appeal ordered an

[31] Case 74742/14 *PIHL v. Sweden* (9 March 2017).

[32] Government-commissioned report (2016:7) "*Integritet och straffskydd*" (February 2016), Chapter 16.

[33] Note that the most prominent Swedish case with respect to online copyright infringement was the landmark judgements against the founders of "The Pirate Bay", see Stockholm District Court in case B 13301-06 (17 April 2009) and Svea High Court (*Svea Hovrätt*) in case B 4041-09 (26 November 2010). This case generated major attention in international media but was limited to criminal proceedings and did not concern any injunction. It is therefore not discussed in this report.

[34] Case PMT 11706-15 discussed above.

ISP to block its users from accessing file-sharing websites involved in copyright infringements for a period of three years.

Although not related to copyright filtering injunctions, we note further that the scope of Article 15 of the E-Commerce Directive as interpreted in the *Scarlet* case,[35] has been discussed in Sweden in relation to the general supervision obligation set in the BBS Act. The Act imposes on online intermediaries a general obligation to supervise their services in order to avoid the occurrence of messages with unlawful content. This supervision shall be "*reasonable considering the extent and objective of the service.*"[36] The preparatory works of the BBS Act clarified that the providers of electronic bulletin boards are not required to review or control every single message in advance. Instead, the supervision obligation may be fulfilled by setting up a simple mechanism whereby users of the service may complain about messages with unlawful content.[37]

The BBS Act was adopted in 1998 and, at the time of implementation of the E-Commerce Directive in 2002, the Government discussed its compliance with Article 15(1) of the Directive which forbids Member States from imposing on intermediaries a general obligation to monitor or to actively investigate illegal activity.[38] The Government found then that the BBS Act did not impose such a general obligation. More recently, a Government-commissioned report found that the *Scarlet* ruling did not alter the conclusion that the BBS Act was in line with Article 15(1) of the Directive.[39]

1.2. Consumer Protection

Question 1.2.1.

The Swedish Consumer Sales Act regulates the non-conformity of goods in the case of sales transactions between a trader and a consumer.[40] In parts, it implements the Consumer Sales and Guarantees Directive (1999/44/EC). In line with the Directive, the Act provides for a variety of remedies in case of non-conformity: repair, replacement, price reduction or having the contract rescinded.

Disputes are handled before the National Board for Consumer Disputes (*Allmänna reklamationsnämnden*) and courts. To the best of our knowledge, there are no major difficulties in applying the rules on remedies set in the Consumer Sales and Guarantees Directive. However, we note that problems may arise in identifying when a seller is acting as a trader or as a private person. This issue,

[35] Case C-70/10 *Scarlet v. SABAM*.
[36] Section 4 of the BBS Act.
[37] Government Bill (1997/97:15), p. 14.
[38] Government Bill (2001/02:150) on the implementation of the E-Commerce Directive, p.100.
[39] See Government-commissioned report (2016:7) "*Integritet och straffskydd*" (February 2016), Chapter 16.
[40] Consumer Sales Act (1990:932) (*Konsumentköplagen*).

which is discussed below,[41] is particularly topical within the collaborative economy.

Another issue which is currently discussed concerns the duration of the presumption under the Consumer Sales and Guarantees Directive and the Swedish Consumer Sales Act. A recent Government-commissioned report on the circular economy found the current six month-period to be too short and proposed to extend it to two years.[42] At this stage, it is unclear whether the report will lead to an amendment of the Act.

Finally, it should be noted that discussions are currently held in Sweden on the appropriateness of extending the protection of consumers in the Consumer Sales Act to certain services.[43] Again, we cannot assess at the time of writing whether these discussions will result in a legislative change.

Question 1.2.2.

Full harmonization of certain aspects concerning contracts for the supply of digital content contributes to the achievement of a digital single market as it removes discrepancies between national legislations. The proposal of the European Commission[44] is therefore a positive step towards further integration.

The Swedish Government has been positive to the Commission's proposal.[45] It noted at the same time, that Sweden does not have specific rules targeting at consumer sales of digital content.[46] Thus, more than harmonizing national rules, the Commission's proposal would have the effect, if adopted, to clarify the rules applying to such transactions in Sweden.

Question 1.2.3.

As for the online sales of goods, full harmonization of certain contractual aspects contributes to the achievement of a digital single market. The proposal of the European Commission[47] is therefore a positive step towards further integration.

[41] See Q 1.4.4, Q 1.4.5 and Q 1.4.6.

[42] Government-commissioned report (2017:22) "*Från värdekedja till värdecykel – så får Sverige en mer cirkulär ekonomi*" (March 2017).

[43] See the Government-commissioned reports with regards to financial advice ("*Det måste gå att lita på konsumentskyddet*", (SOU 2014:4)), consumer credits ("*Stärkt konsumentskydd på marknaden för högkostnadskrediter*", (SOU 2016:69)) and sales via telephone ("*Ett stärkt konsumentskydd vid telefonförsäljning*", (SOU 2015:61)).

[44] COM(2015) 634 final.

[45] Government PM "*Direktiv om avtal för tillhandahållande av digitalt innehåll*" (2015/16:FPM36), 11 January 2016.

[46] General contract law provisions would currently apply to such transactions.

[47] COM(2015) 635 final.

The Swedish Government is supportive of this initiative but expressed concerns that it may lead to regulatory divergence between online and offline sales.[48]

Indeed, the Commission's proposal provides for a specific regime for online sales which may differ from existing rules applying to traditional sales in brick-and-mortar shops. Applying different rules to online and offline transactions may not necessarily be an issue. However, we note that the development of omni-channel strategies by retailers blurs the demarcation between online and offline sales. In the case of hybrid sales, which combine both online and offline elements,[49] it may sometimes be challenging for the consumer and for the trader to identify which rules would apply.[50] It is therefore important for any new legislation to take into account these market developments in order to avoid unclear or unpractical rules.

Question 1.2.4.

The European Commission recently presented its evaluation of the EU consumer protection legislation.[51] We have no reason to question the Commission's findings. We note further that consumer confidence in cross-border transactions is not only dependent on the mere existence of harmonized rules. Factors such as consumer awareness of their rights, general trust in online sales channels (e.g. trust in secured payment systems and in the respect of one's privacy), availability and pricing of parcel delivery as well as cultural preferences also play a role in boosting consumer confidence for cross-border e-commerce.

Not all of these factors can be addressed by way of harmonization and, although it is clear that EU consumer protection legislation contributes to the achievement of a digital single market, its real impact on B2C online trade may be difficult to evaluate.

Question 1.2.5.

The role of online platforms has become increasingly important in the rise of the collaborative economy whereby consumers buy goods and services from other users. As noted below,[52] consumer rules (both at EU and national levels) would only apply to such transactions if the sellers of goods or services qualify

[48] Government PM "*Direktiv om försäljning av varor på nätet eller annars på distans*" (2015/16:FPM37), 11 January 2016.

[49] For instance ordering a good online and collecting it in a brick-and-mortar shop.

[50] For a similar reasoning with regards to the right of withdrawal under the Consumer Rights Directive (2011/83/EU), see Section 3.4.4 of National Board of Trade "Online Trade, Offline Rules – A Review of Barriers to E-Commerce in the EU" (2015:7), May 2015.

[51] SWD(2017) 209 final, SWD(2017) 169 final and COM(2017) 259 final, 23 May 2017.

[52] See Q 1.4.4, Q 1.4.5 and Q 1.4.6.

as "traders". Conversely, the consumer rules would only apply to the relationship between the online platform and the sellers of goods or services if the latter qualify as "private individuals".

The scope of application of EU consumer protection law is therefore subject to a case-by-case analysis. This analysis may be challenging for the users of platforms as they are not always aware of the legal status of the party selling goods or services. This is all the more challenging in the case of cross-border transactions for which the assessment of the legal status of a user under foreign consumer rules may be even more problematic.

As much as it is important to provide for harmonized rules in the field of consumer protection, it is also necessary to make sure that consumers are well informed about their rights and obligations.

In that respect, online platforms play an important role in informing their users about applicable consumer rules. A recent Government-commissioned report noted however that online platforms in Sweden do not always provide adequate information to their users.[53] The survey presented in this report shows for instance that price information or contact information on platforms is sometimes lacking or is not sufficient and that the terms and conditions do not always clearly inform the users about their respective rights and obligations.

Question 1.2.6.

There is an extensive case-law on the application of the Swedish Consumer Contracts Act[54] which in turn implements the Directive on Unfair Contract Terms (93/13/EEC).

With regards to platforms, an interesting example concerns the termination clauses of an online dating site. The Consumer Ombudsman (*Konsumentombudsmannen*)[55] had brought an action before the Market Court (*Marknadsdomstolen*) arguing that both the formal requirements for termination (by way of de-registration or by letting the account dormant for 12 months) and the duration of the termination notice (60 days) were unfair.

The Market Court followed the line of the Consumer Ombudsman and found that both conditions were in breach of the Consumer Contracts Act.[56] With regards to the first issue, Swedish law does not explicitly address the form of termination, but the Market Court referred to earlier cases related to the telecom market in which the requirements of a written termination notice were found to

[53] Government-commissioned report (2017:26) "*Delningsekonomi – På användarnas villkor*" (March 2017).
[54] The Consumer Contracts Act (1994:1512) (*Lagen om avtalsvillkor i konsumentförhållanden*).
[55] The Consumer Ombudsman is a part of the Swedish Consumer Agency (*Konsumentverket*). It is entrusted with the task of bringing certain consumer-related complaints before the Swedish courts.
[56] Market Court in case MD 2015:3 (9 March 2015).

be unfair. With regards to the second issue, the Market Court applied the general consumer law principle according to which termination notice shall not exceed one month unless otherwise motivated.

Question 1.2.7.

Consumer protection legislation aims at correcting imbalances between consumers and traders. To the extent that similar imbalances are observed in Business to Business (B2B) relationships, notably between online platforms and their professional users, it is legitimate to discuss the appropriateness of introducing a certain level of protection for the weaker party, here the users of platforms.

In its mid-term review of the implementation of the DSM Strategy, the European Commission announced its ambition to address, by the end of 2017, issues related to unfair trading practices in platform to business relationships.[57] The Commission referred to the preliminary results of a fact-finding exercise indicating practices which are detrimental to professional users. The examples provided by the Commission included the delisting of products or services without notice, platforms favoring their own products and services, the lack of transparency in the platforms' ranking or search results and the lack of accessible and effective redress mechanisms.

We have not had access to the Commission's fact-finding exercise and find it therefore difficult to assess whether clauses and practices which were provided as examples by the Commission are indeed "unfair", and if so on which grounds, and whether they could be tackled by existing rules (e.g. the Services Directive (2006/123/EC) or the EU competition rules).[58] Nor can we approximate the extent of the alleged problems and if so whether they should be better addressed in binding EU rules or in self-regulatory codes of conduct.

With regards to Sweden, we note that Swedish-based Spotify has in several instances complained about Apple's subscription policy which, Spotify argued, would favor the platform's own services.[59] It is for us unclear whether such policy, if confirmed, would constitute a violation of the EU competition rules (Article 102 TFEU).

[57] COM(2017) 228 final, p. 8-9.

[58] Several of the examples provided by the Commission in its mid-term review may for instance be tackled by the EU competition rules (Article 102 TFEU) in so far as the platform would be found to hold a dominant position. Such finding may however be difficult to assess. In that respect, it may be appropriate to consider the concept of "abuse of economic dependency" which, in several EU countries, supplements the prohibition of "abuse of dominant position" and may be more adapted to the digital economy where market shares do not always reflect the competitive situation on a market.

[59] See for instance recode.net "Spotify says Apple won't approve a new version of its app because it doesn't want competition for Apple Music" (30 June 2016).

1.3. Geo-Blocking

Question 1.3.1.

In its proposal for a Regulation on geo-blocking,[60] the Commission mentions that the non-discrimination provision in the Services Directive has proven difficult to enforce in the EU. Sweden is no exception and, to the best of our knowledge, Section 20 of the Internal Market Services Act[61] which implements Article 20 of the Services Directive has not been discussed in Swedish case-law.

Although the Swedish official position was positive to the Commission's proposal, the Swedish Government was also keen to stress the importance of balancing consumer protection with the freedom of contract and the freedom to conduct a business.[62] As far as we know the relation between the proposed regulation and the Brussels I Regulation (1215/2015/EU) has not been publicly discussed in Sweden.

In that respect, we note that the Commission's proposal states that the prohibition of geo-blocking and of discriminatory practices "*shall not be construed as implying that a trader directs his or her activities to the Member State where the consumer has the habitual residence or domicile*" (Article 1(5)). The CJEU has provided some guidelines for assessing when a trader is directing its activities to another Member State.[63] Such assessment is made on a case-by-case on the basis of a number of factors. An online trader or a consumer may therefore not always easily identify which national rules apply to a given transaction. There is in our view a risk that the obligation to sell to a consumer in another Member State makes such assessment even less predictable.

In spite of Article 1(5) of the proposed Regulation on geo-blocking it is likely that traders would have to be cautious in handling transactions with consumers in Member States to which they have no intention to sell. Conversely, consumers may face difficulties in assessing whether a transaction is the result of a commercial decision by the trader or is merely imposed by the proposed prohibition of discrimination.[64]

[60] Proposal for a Regulation on addressing geo-blocking (COM(2016) 289 final), 25 May 2016.

[61] Internal Market Services Act (2009:1079) (*Lag om tjänster på den inre marknaden*).

[62] See for instance comments made by the Swedish minister Ann Linde with regards to the Council meeting on e-commerce and patent (25 November 2016).

[63] See joined cases C-585/08 and C-144/09 *Pammer* and *Hotel Alpenhof*.

[64] Similar difficulties may arise with the presentation of an offer which may be intended by the trader or forced by the prohibition on geo-blocking.

1.4. Collaborative Economy

Question 1.4.1

The emergence of the collaborative economy raises a number of legal and competition issues. The debates in Sweden has not been as heated as in some other EU States but the novelty of this phenomenon calls for a clarification of the regulatory framework. Among the issues discussed in Sweden are the risk of unfair competition posed by platforms such as Uber and Airbnb and the rights of consumers in buying goods or services from peers via online platforms. We examined these two issues below.

Question 1.4.2.

In a number of sectors, the emergence of online platforms puts pressure on traditional businesses. This is for instance the case with the hotel industry facing competition from platforms such as Airbnb and taxis which are competing with peer-to-peer services such as Uber. As in many other EU countries, traditional operators argue that the emergence of the collaborative economy distorts competition as online platforms are not subject to the same regulatory framework. By avoiding certain labor, tax and other regulatory requirements, traditional businesses argue, online platforms are able to offer competing services at a lower cost.

The reality is however more nuanced. In the case of Uber for instance, a recent ruling qualified the peer-to-peer service of Uber Pop as a taxi activity and condemned a driver for failing to hold a proper taxi license.[65] As a result, Uber withdrew its Uber Pop services from the Swedish market.

With regards to carpooling platforms, a recent Government-commissioned report, clarifies that it falls outside the scope of the rules on taxi businesses as long as the car owner or the driver does not make a profit of its activity.[66] In order to avoid abuses, the report states further that it may be necessary in the future to subject online platforms providing carpooling services to an authorisation or a notification requirement.[67]

As for platforms providing accommodation, such as Airbnb, Swedish law does not impose any specific restrictions. However, in practice, the rental of an apartment is subject to the approval by the landlord (in the case of tenancies) or by the association of owners (in the case of owner-occupied dwellings).[68] For instance, in a case related to the rental of an apartment via Airbnb in Stockholm, the regional Rent Tribunal (*Hyresnämnden*) ruled that the owner was not allowed to rent her

[65] Svea Court of Appeal in case B 9078-15 (23 March 2016).

[66] Government-commissioned report (2016:86) "*Taxi och samåkning*" (November 2016).

[67] As far as we know, this issue has not been discussed further by the Swedish legislator.

[68] Tenancies and owner-occupied dwellings being the main accommodations in urban areas.

apartment without the approval of the association of owners.[69] Given the nuisance which co-owners may experience with regards to repeated short-term rentals within their apartment building, the obligation to obtain one's neighbours' approval amounts to more than a mere formality.

More generally, a recent report by the Swedish Competition Authority (*Konkurrensverket*) noted that there were competition issues related to the emergence of the collaborative economy.[70] Its conclusions however were that the current competition rules were "*well suited to deal with competition-related problems that may occur with these new services.*" (p.11). The Authority did on the other hand point out the need to consider new thresholds for merger control as the turnover of e.g. online platforms at the time of such transactions does not necessarily reflect their market power.

Question 1.4.4.

Transactions via online platforms involve three parties: the users, i.e. the person providing a service or a good and the person buying or renting the service or good in question, and the platform itself. Thus such transactions result in three contracts being concluded: between the users themselves and between each user and the platform.

This three party relationship raises in turn consumer protection issues. As mentioned above, when the person providing a service or a good qualifies as a "trader", the contract between the users is subject to the Swedish consumer rules, the Consumer Protection Act and the Consumer Services Act.[71] In practice this means that a number of obligations on e.g. pricing, information and dispute resolution are imposed on the trader. Those obligations do not however apply if the person providing a service or a good qualifies as a private individual.

A recent Government-commissioned report examined the concept of "trader" within the context of the collaborative economy.[72] This covers "*all physical or legal persons who run an economic operation of a certain size and duration and of such character that it may be designed as professional*" (p.39). Given this elastic definition, a case-by-case assessment is required in order to assess whether a supplier of goods or services qualifies as a trader. The delineation between a trader and a private individual is not always obvious for the person concerned, and even less for the counterparty. For instance, a retired professional painter may under certain circumstances qualify as a "trader" if he is providing painting services on a regular

[69] Stockholm Rent Tribunal in case 8741-15 (17 August 2015).

[70] Swedish Competition Authority (2017:2) "*Konkurrens och tillväxt på digitala marknader – ett regeringsuppdrag om e-handel och delningsekonomi*" (1 March 2017).

[71] Consumer Protection Act (1990:932) (*Konsumentköplagen*) and Consumer Services Act (1985:716) (*Konsumenttjänstlagen*).

[72] Government-commissioned report (2017:26) "*Delningsekonomi – På användarnas villkor*" (March 2017).

basis. He would on the other hand qualify as a "private individual" if his services are limited to a single transaction.

Note that the same issue arises in the relationship between the provider of goods or services and the platform. The latter qualifies as a trader and as such is subject to the Swedish rules on consumer protection, but only to the extent that the user does not qualify as a "trader".

The report did not however propose legislative changes to clarify this issue. It did note that the extent of the problem is still limited given the novelty of this phenomenon and called for a regular overview of the collaborative economy. It also proposed that the Swedish Consumer Agency (*Konsumentverket*) be tasked with providing independent information and guidance on e.g. the legal status of users involved in the collaborative economy.[73]

2. Digital media

Question 2.1.

Swedish practice is in line with the interpretation of the AVMS Directive (2010/13/EU) made by the CJEU in the *New Media Online GmbH* case.[74] Prior to that ruling, the Swedish Broadcasting Commission (*Granskningsnämnden* or "**SBC**")[75] had already found that the provision of on-demand videos under the subdomain of a newspaper's website qualified as an "audiovisual media service".[76] More specifically, the SBC considered that the prohibition for certain programmes to improperly promote commercial interests applied to three videos presented on the website of the evening newspaper Aftonbladet. That finding was based on the interpretation of the Swedish Radio and TV Act,[77] itself an implementation of the AVMS Directive, and was not disputed before court.

More recently, the SBC confirmed this view with explicit reference to the *New Media Online GmbH* ruling in a case involving on-demand videos presented on the website of a commercial TV-channel (TV4).[78]

Question 2.2.

The BBS Act described above applies in principle to video-sharing platforms to the extent that they are not already protected under the rules on the freedom of

[73] To the best of our knowledge, the Government is yet to adopt a position on this issue.

[74] Case C-347/14 *New Media Online GmbH v. Bundeskommunikationssenat*.

[75] The SBC is an independent body within the Swedish Press and Broadcasting Authority (*Myndigheten för press, radio och tv*). The SBC reviews the compliance of the contents of radio and TV programmes with the Swedish broadcasting regulations.

[76] See for instance the SCB decision in case 12/00778 (29 October 2012).

[77] Radio and TV Act (2010:696) (*Radio- och tv-lagen*).

[78] SCB decision in case 16/00243 (16 May 2016).

expression. Thus it should be possible under Swedish law to order such platform to remove messages (including videos) which incite to racial hatred or contain unlawful depiction of violence. As mentioned however, this law has been criticized for its narrow scope of application and its lack of clarity. In any case, it is unlikely that it would trigger the liability of platforms established outside Sweden. To the best of our knowledge, the issue has not been tested before the Swedish courts.

The Swedish Government has been critical of the Commission's proposal to bring video platforms under the scope of the AVMS Directive.[79] In particular, the Government stressed the need to secure a broad freedom of expression and of information and an open and free internet. Further it called for a clear and restrictive definition of the concept of "video-sharing platforms" to be included.[80]

The subsequent broadening of this definition to include social media services "*if the proportion of audiovisual content is significant to the main activity or other activities of that service*"[81] has been criticized by a number of Member States, including Sweden.[82] Together with six other Member States, Sweden sent an unpublished non-paper to the EU Council presidency stressing the problem of requiring platforms to "*"police" non-illegal content over which they do not have editorial control*".[83]

As a general comment, it may be debatable whether the AVMS Directive which targets at media service providers with editorial responsibility is suitable to address issues raised by media without such responsibility. As mentioned above, the liability of intermediaries is regulated in a wide variety of EU legal acts and a horizontal approach might be more appropriate to tackle problems related to e.g. hate speech.[84] Such horizontal approach would have the merit of weighing in conflicting interests such as the freedom of speech and the fight against illegal content by taking into account the role(s) of intermediaries in a technologically-neutral way.

Question 2.3.

In the early years of the first AVMS Directive (89/552/EEC), the Swedish Market Court raised the issue of the scope of the country-of-origin principle with regards to television broadcasts from other Member States. This question was

[79] COM(2016) 287 final (25 May 2016).

[80] Government Promemoria 2015/16:FPM101 (29 June 2016).

[81] Council review of the Commission's proposal 8242/17 (24 April 2017).

[82] For instance, see Sweden's joint call with Czech Republic and Iceland to ensure "*that the provisions in relation to the definitions are legally sound and clear in order to avoid stifling freedom of expression and suppressing innovation in this key area*." Council draft minutes 9547/17 (13 June 2017).

[83] According to European Digital Rights "AVMS Directive: It isn't censorship if the content is mostly legal, right?" (27 April 2017), available on www.edri.org.

[84] As an example of horizontal (non-binding) approach, see the Commission's communication on "Tackling Illegal Content Online" (COM(2017) 555 final).

referred to the CJEU which, in the *De Agostini* case,[85] stated that Swedish broadcasting rules precluding television advertising directed at minors could not apply to television broadcasts from other Member States. To the best of our knowledge, the country-of-origin principle has not been discussed before the Swedish courts in the last years.

However, in recent years, discussions have been held in Sweden with respect to television advertising of alcohol products by broadcasters established in the UK. The Swedish broadcasting rules on alcohol are stricter than in most Member States as they prohibit all forms of television advertising.[86] In accordance with the AVMS Directive, these rules do not apply to broadcasters established in other Member States.[87]

Thus the broadcasters Viasat and SBS, both of which have headquarters in London but are targeting at a Swedish audience,[88] are subject to the more lenient UK rules which allow them to provide alcohol advertising. The Swedish Press and Broadcasting Authority (*Myndigheten för press, radio och tv* or "*SPBA*") is of the view that Viasat and SBS have been established in the UK in order to circumvent the stricter Swedish rules on alcohol advertising. It has therefore initiated proceedings in accordance with the consultation procedure set in Articles 4(2), 4(3) and 4(4) of the AVMS Directive.

In late 2014, following contacts with the UK Broadcasting Authority (Ofcom) and discussions with Viasat and SBS, the SPBA notified the European Commission and Ofcom of its intentions to take actions against the two broadcasters.[89] Without taking position on the EU law analysis made by the SPBA, the Commission asked for clarifications of the Swedish position. As a result, and given the tight deadline set in Article 4(5) of the AVMS Directive, the Swedish Authority decided to withdraw its notification letter in February 2015.[90]

From our contacts with the SPBA, we understand that the matter is not closed at the time of writing and that a new notification is expected to take place within the coming months.[91] We note that it is likely that Brexit will act as a game-changer on this issue.

[85] Joined cases C-34 to 36/95 *De Agostini*.

[86] The Radio and TV Act and the Law on Alcohol (2010:1622) (*Alkohollagen*).

[87] See Chapter 1, Section 3 of the Swedish Radio and TV Act.

[88] The programs of Viasat Broadcasting UK Limited (with the channels TV3, TV6 and TV8) and SBS Discovery Media UK Limited (with the channels Kanal 5 and Kanal 9) are either in Swedish or with Swedish subtitles.

[89] Notification letter (11/00567) of the SPBA to the European Commission and Ofcom (19 December 2014).

[90] Withdrawal letter (11/00567) of the SPBA to the European Commission and Ofcom (6 February 2015).

[91] Aside from this case, the SPBA has concluded a cooperation agreement with Ofcom which, in practice means that the Authority forwards complaints related to London-based broadcasters to its counterpart

Question 2.4.

The Swedish Press and Broadcasting Authority is a government agency under the Ministry of Culture. Its independence is guaranteed by a fundamental law which has constitutional value.[92] To our knowledge, neither the Government, nor the Parliament have intervened to influence its decisions.[93]

It is therefore unlikely that the introduction of independence requirements at EU level would significantly alter the position of the Swedish media regulator.

Question 2.5.

Over the years, the Swedish broadcasting rules have been successively adjusted in order to adapt to the development of digital media. Issues such as the extent of the freedom of speech, competition from new forms of digital media or the territorial application of these rules have thus regularly been discussed in Sweden. Specific problems such as the alleged circumvention of the Swedish ban on television advertising for alcohol products mentioned above are still unresolved. Similarly, the impartiality and financing of public service operators is repeatedly debated in the political arena.[94]

With regards to further harmonisation, the Swedish Government has been critical of several of the points introduced in the Commission's latest proposal. Aside from the new rules on video-sharing platforms discussed above, the Government also objected to too detailed requirements regarding national regulators as well as the new quotas proposed by the Commission.[95]

Question 2.6.

Television advertising targeting at minors under the age of 12 is banned under the Swedish broadcasting rules.[96] The ban includes on-demand services but does not apply to media service providers established in other Member States. For broadcasters with headquarters in London (see above), the more lenient UK rules on television advertising apply.

in the UK. The number of complaints increased from 25 in 2015 to 45 in 2016. See the Annual Report (2016) of the SPBA, p. 21.

[92] See Chapter 12, Section 2 of the Instrument of Government (1974:152) (*Regeringsformen*).

[93] To the question whether there have been recent legislative or governmental interventions with potential impact over its decisions, the SPBA answered negatively. See the report of the European Regulators Group for Audiovisual Media Services (ERGA) on the independence of National Regulatory Authorities (11 January 2016), p. 56.

[94] For instance, see some latest op-eds in Swedish newspapers: "*Cwejman: Statlig media är aldrig oberoende*" Göteborgs-Posten (30 May 2017), "*Finansiera inte public service via skattsedeln*" Svenska Dagbladet Debatt (15 September 2017) or DN Debatt. "*Inkomstbaserad tv-licens kan sänka public service*" (31 August 2017).

[95] Government Promemoria 2015/16:FPM101 (29 June 2016).

[96] See Chapter 8, Section 7 of the Radio and TV Act.

Aside from this general ban on television advertising, the Personal Data Act, which implements the Personal Data Directive (95/46/EC), requires the consent of the data subject for the processing of his or her personal data.[97] This affects targeted marketing or personalized content for which consent must have been granted by the targeted data subject.[98]

To the best of our knowledge, no other rules apply to the offering of targeted (or addressable) advertising on television or of personalised content in Sweden. Nor are we aware of any initiative from the Swedish DPA (*Datainspektionen*) or the Swedish Press and Broadcasting Authority in that field.

Question 2.7.

The development of online transmissions has rendered the Satellite and Cable Directive (93/83/EEC) less relevant in Sweden. The clearance mechanism set in the Directive does not apply to online transmissions of broadcasting organisations. The Commission's proposal in that area[99] would therefore require, if adopted, changes in the Swedish Copyright Act.

Question 2.8.

As for many other EU countries, the main obstacles to cross-border portability of digital content in Sweden are not regulatory ones. Copyright issues, notably the cost-benefit of clearing rights in multiple jurisdictions, is probably the single most important reason for limited portability.[100]

This issue is partly addressed by the newly-adopted Regulation on cross-border portability of online content services (2017/1128/EU). The Regulation imposes an obligation for online content service providers to enable such portability at no extra cost for paying subscribers who are temporarily present in another Member State.[101] The Regulation further provides for compliance of the verification mechanisms with the EU rules on data protection, and we therefore do not foresee any conflict with the data minimisation principle.

The Regulation will apply in Sweden and the rest of the EU from 1 April 2018. It is unclear at the time of writing if supplementary rules will be adopted at national level.

[97] Note that the Swedish rules on data protection are examined more in detail under Section 4 below.

[98] Note that both the Personal Data Act (Section 11) and the Marketing Act (Section 19) contain specific restrictions on direct marketing.

[99] Commission proposal for a Regulation on copyright and related rights applicable to online transmissions of broadcasting organisations and retransmissions of television and radio programmes, COM(2016) 594 final (14 September 2016).

[100] See for instance National Board of Trade "Online Trade, Offline Rules – A Review of Barriers to E-Commerce in the EU" (2015:7), Section 4.3.

[101] In the case of non-paying subscribers, providers may opt for such portability.

3. Digital Infrastructures

Question 3.1.

Since the entry into force of the TSM-Regulation (2015/2120/EU), the Swedish NRA (*Post- och telestyrelsen*) has been supervising traffic management by ISPs, mostly on the mobile market. In particular, it adopted a decision prohibiting zero-rating practices by one operator (Telia) and imposed conditions on other such practices by another operator (Hi3G).

The *Telia* case concerns subscriptions whereby the use of certain applications (social media in one case and music and radio streaming in the other) is not subject to the data cap included in those subscriptions. Thus, when the data cap is reached, Telia blocks the possibility for users to surf online except for the selected applications. In line with the EU guidelines on net neutrality,[102] the Swedish NRA found that this practice amounted to traffic management prohibited by the non-discrimination provision set in Article 3(3) of the TSM-Regulation. It therefore ordered Telia to discontinue such traffic management.[103]

This decision was appealed by Telia and, in March 2017, the Administrative Court of Appeal (*Kammarrätten*) granted Telia interim relief pending final judgment.[104] Given the Court's mention of the lack of guidance for interpreting the TSM-Regulation, it is not unlikely that a reference for a preliminary ruling is made to the CJEU in the coming months.

The *Hi3G* case concerns mobile internet subscriptions whereby users can stream selected music applications without it affecting the data volume included in the subscription. Unlike the *Telia* case however, Hi3G agreed to follow the Swedish NRA's interpretation of Article 3(3) of the TSM-Regulation and to adjust its offer accordingly. According to the Swedish NRA, until the data cap is reached, users may still use the zero-rated applications without this traffic being deducted from the agreed data volume. However, once the data cap is reached, Hi3G has agreed to discontinue the differential treatment.[105] This case illustrates the view of the Swedish NRA which is to prohibit traffic management resulting in cer-

[102] Body of European Regulators of Electronic Communication (BEREC) "Guidelines on the Implementation by National Regulators of European Net Neutrality Rules" BoR (16) 127 (August 2016), paragraph 55.

[103] See the Swedish NRA decision in cases 16-5475 and 16-5476 (24 January 2017).

[104] Administrative Court of Appeal in case 1178-17 (8 March 2017). Note that in first instance the Administrative Court (*Förvaltningsrätten*) had rejected Telia's appeal for interim measures on the grounds that it was likely that the Swedish NRA had acted correctly, see case 4207-17 (22 February 2017). The Administrative Court of Appeal overruled that judgment and stressed that, in addition of the irreparable damages incurred by Telia, the outcome of the case was uncertain as the TSM-Regulation was a new instrument and that there was little guidance on how it should be interpreted.

[105] See the Swedish NRA "Net neutrality report 2016/2017 – Report to the European Commission and BEREC according to Regulation (EU) 2015/2120" PTS-ER-2017:15 (26 June 2017), p. 24-25.

tain applications being accessible when others are not, rather than banning all zero-rating practices.

Both the *Telia* and *Hi3G* cases relate to the interpretation of Article 3(3) of the TSM-Regulation. The Swedish NRA also recently launched new inquiries which seem to relate to the application of Article 3(2) of the Regulation.[106] At the time of writing, the scope of these fact-finding inquiries is still unclear and it is too early to assess whether they may result in the Swedish NRA adopting a specific position on the rights of end-users.

Question 3.2.

The Broadband Directive (2014/61/EU) was implemented in Sweden via the Law concerning proceedings for the expansion of broadband infrastructure.[107] This law provides for access to network infrastructure for operators which are deploying a broadband network.[108] It further obliges procurement authorities to integrate the building of a broadband network in their construction projects.

These measures are in line with the new Broadband Strategy adopted by the Swedish Government in December 2016.[109] This strategy aims at a "*completely connected Sweden by 2025*". The short-term goal of the strategy is for 95 percent of all households and businesses to have broadband access at a minimum capacity of 100 Mbit/s by 2020. By 2025, the Government aims at 98 percent of the population having access to a capacity of 1 Gbit/s whereas the remaining 1.9 percent would have access at a capacity of 100 Mbit/s and the last 0.1 percent at a capacity of 30 Mbit/s. These targets constitute an upgrade compared to those set in the previous Broadband Strategy (2009) and are well in line with those presented by the European Commission.[110]

In that respect, the Government announced that it was actively contributing to the Commission's overhaul of the regulatory framework for electronic communications and aimed at adopting clearer and simpler rule in order to facilitate investment in broadband infrastructures. The Government also announced that it was supporting municipalities in the development of local network infrastructures, for instance by removing regulatory obstacles related to permit processes.

[106] See the Swedish NRA's press release "*PTS begär in information relaterad till nätneutralitetsregler*" (15 May 2017).

[107] Law concerning proceedings for the expansion of broadband infrastructure (2016:534) (*Lagen om åtgärder för utbyggnad av bredband*).

[108] A similar obligation is imposed on property owners in accordance with an amendment of the Electronic Communication Act (2003:389) (*Lagen om elektronisk kommunikation*).

[109] Government report "A Completely Connected Sweden by 2025 – a Broadband Strategy" (21 December 2016).

[110] European Commission "State of the Union 2016: Commission paves the way for more and better internet connectivity for all citizens and businesses" (14 September 2016).

With regards to 5G, whose development is another priority of the European Commission, the digitization ministers of the Nordic and Baltic countries agreed to draw up a common development plan in April 2017.[111] It is however unclear whether the 2020-target set by the Commission will be reached. In that respect, we note that some private operators have already announced their intentions to offer "5G-experience" in Stockholm by 2018.[112]

Question 3.3.

The Swedish NRA is an independent authority which manages the radio spectrum by i.a. allocating radio frequencies to operators in accordance with the Electronic Communications Act.[113] In line with the Authorization Directive (2002/20/EC), the Swedish NRA strives "*for a high degree of transparency and competition neutrality, applying "objective, transparent, non-discriminatory and proportionate criteria" in selection procedures*".[114] In a few cases, decisions to allocate frequencies have been appealed before courts[115] but we are not aware of any situation where a court would have quashed such decisions.

In October 2016, the Swedish NRA withdrew a spectrum auction for the 700 MHz band (with potential use for 5G) due the Government's concerns that part of the spectrum may be requested for use by the military, ambulances and other operators within public order, health, safety and defence.[116] After further inquiry, the Swedish Government authorized the NRA to proceed with the auction which is scheduled to be held in November 2017.

In that context, one private mobile operator complained in the media that the NRA was favouring the partly State-owned operator Telia in limiting the number of authorizations to be granted in this process.[117] Under the new auction, only two authorizations would be granted for a market comprising four mobile operators which, the private operator argued, would limit competition.[118] We have no indication that these accusations would be substantiated and note that

[111] Nordic Council of Ministers "The Nordic-Baltic region: a digital frontrunner" (25 April 2017).

[112] TeliaSonera press release "TeliaSonera and Ericsson Go 5G", see also IDG.se "*Stora oklarheter runt Telias 5g-löfte till Stockholm*" (22 January 2016) and "*Peter Eriksson: Sverige ska leda 5G-utvecklingen i Europa*" (28 February 2017).

[113] Chapter 3 of the Electronic Communications Act.

[114] Swedish NRA "PTS Swedish Spectrum Policy" (PTS-ER-2014:16) (15 April 2014), p. 42.

[115] For instance, appeals brought before the administrative courts by Nordisk Mobiltelefon International, see Administrative Court of Appeal in case 815-10 (7 July 2010) or Stockholm Administrative Court (*Länsrätten*) in case 7281-12 (26 September 2012).

[116] Swedish NRA decision in case 15-6916 (31 October 2016).

[117] Dagens Industri "*Operatören 3: Staten ger Telia en gräddfil i 5g-nätet*" (26 June 2017).

[118] The previous auction which was interrupted in October 2016 covered three authorizations.

the Swedish NRA has plainly rejected them.[119] At the time of writing, no legal action has been taken against the Swedish NRA.

4. Data in the global economy

Question 4.1.

The main Swedish law on the protection of personal data is the Personal Data Act which, as mentioned above, implements the Data Protection Directive. The replacement of the Directive by the General Data Protection Regulation (2016/679/EU) or "*GDPR*", means that the processing of personal data is now regulated at EU level. Yet, even if the Personal Data Act will be repealed by May 2018, a number of national rules will still be necessary in order to complement the GDPR.

In Sweden, a dozen of inquiries have been commissioned by the Government to assess the need for such national rules.[120] The main report, presented to the Government in May 2017, proposes a new Data Protection Act containing supplementary provisions to the GDPR.[121] This new law would for instance provides for the application of certain provisions of the GDPR to activities which fall outside the scope of the GDPR, i.e. the processing of personal data covered by the EU Common Foreign and Security Policy.

The report also proposes a general exemption from the GDPR for the processing of personal data which falls within the scope of the Fundamental Law on Freedom of Expression and the Freedom of the Press Act (see below, Section 4.2).[122] This is complemented by an exemption for the processing of personal data for journalistic purposes or for academic, artistry or literary expression. A final exemption covers the processing of personal data which falls within the scope of the Swedish principle of public access to official documents (*Offentlighetsprincipen*). The report finds that such exemptions are in line with Articles 85 and 86 of the GDPR.

[119] Dagens Industri "*PTS: Vi ser till konsumentnyttan*" (26 June 2017).

[120] For instance for adapting the rules on national courts (Report "*En omarbetad domstolsdatalag – Anpassning till EU:s dataskyddsförordning*" (Ds 2017:41, August 2017)), taxation and customs (Report "*EU:s dataskyddsförordning: Anpassade regler om personuppgiftsbehandling inom skatt, tull och exekution*" (Fi2017/02899/S3, June 2017)), elections (Report "*Anpassning av lagen (2001:183) om behandling av personuppgifter i verksamhet med val och folkomröstningar till dataskyddsförordningen*" (Ju2017/05728/L6) (July 2017)), education (Report "*EU:s dataskyddsförordning och utbildningsområdet*" (SOU 2017:49, June 2017) and research (Report "*Personuppgiftsbehandling för forskningsändamål*" (SOU 2017:50, June 2017)).

[121] Government-commissioned report (2017:39) "*Ny dataskyddslag*" (May 2017).

[122] The Fundamental Law on Freedom of Expression (1991:1469) (*Yttrandefrihetsgrundlagen*) and the Freedom of the Press Act (1949:105) (*Tryckfrihetsförordningen*).

The report also proposes a number of supplemental measures in the new Data Protection Act, from lowering the age of consent of minors to 13 years[123] to the powers of the Swedish DPA. At the time of writing, we understand that the Government is still considering the proposals put forward in this inquiry before presenting a bill to the Parliament.

Question 4.2.

At the time of writing, it is too early to describe the measures taken, or to be taken, by businesses in order to comply with the GDPR. Our understanding is that most companies are still considering ways to adapt their operations to the new EU rules. A number of guidelines have been provided by the Swedish DPA[124] and trade organisations[125] and courses and seminars are regularly offered to companies. Several operators are providing services to companies and public authorities in order to identify potential compliance issues and implement routines in line with the GDPR and/or outsource the Data Protection Officer's function.

Free Speech and Data Protection

A separate issue, which is not specific to the GDPR, relates more generally to the relationship between data protection in Sweden and the freedom of speech. As mentioned the freedom of speech is protected under the Fundamental Law on Freedom of Expression and the Freedom of the Press Act, both of which have a constitutional value. In practice, this means that the Personal Data Act (and as of May 2018, the GDPR) does not apply to persons falling within the scope of the Swedish rules on the freedom of speech.

This concerns mass media companies which enjoy automatic protection as well as any Swedish person who has applied for, and obtained a so-called "publishing certificate" (*Utgivningsbevis*).[126] A number of Swedish actors have been granted such certificates and, as a result, are exempted from the requirements set in the Data Protection Act. They can therefore provide personal information to their users without the consent of the data subjects.

[123] Under the GDPR, children must be 16 to give their own consent to the processing of personal data in relation to certain information society services (Article 8). Member States may however lower that age limit to 13.

[124] Guidelines for data controllers ("*Förberedelser inför EU:s dataskyddsförordning – Vägledning till personuppgiftsansvariga*") and for data processors ("*Vägledning för personuppgiftsbiträden*"). Both are available on the website of the Swedish DPA (www.datainspektionen.se).

[125] For instance the Confederation of Swedish Enterprises published a guide with advices on how to comply with the GDPR ("*Företagen och dataskyddsförordningen – Nya regler för hantering av personuppgifter*") available on the organization's website (www.svensktnaringsliv.se).

[126] Such certificate is issued by the SPBA subject to certain condition, for instance that there shall be a responsible editor.

Swedish media have for instance discussed a website where subscribers can search if a given person has been convicted of a crime.[127] The website makes available electronic copies of judgements which are hereby made easily accessible to anyone for less than € 10 per month. Other websites provide search functions which enable users to check the address, income or marital status of given persons.

The Swedish DPA is barred from monitoring these websites as they are protected under the rules on the freedom of speech. A recent Government-commissioned report proposed to amend those rules and to exclude the provision of certain sensitive data (e.g. health data, political opinions or criminal convictions) from the scope of the Fundamental Law on Freedom of Expression and the Freedom of the Press Act.[128]

It is still unclear if, and to which extent, the rules on freedom of speech will be amended. However, the Swedish DPA recently informed the Government that, in any case, the problems of non-sensitive data would still remain.[129] In particular, the DPA highlighted a complaint it had received from an Austrian citizen, Mr. Max Schrems, who argued that the Swedish mobile application "Truecaller" had made available to its users his phone number without his consent.[130]

Truecaller holds a publishing certificate and is therefore not subject to the Personal Data Act even though its business is not primarily concerned with free speech. The Swedish DPA expressed its concerns that the generous rules on free speech may restrict the level of privacy protection set at EU level.[131] Aside from the case of Truecaller, the DPA referred to the "countless number of complaints" it had received on this issue to call for a more ambitious reform of the Swedish rules and to allow it to monitor search engines which today hold a publishing certificate.

[127] For example Expressen.se: "*Deras liv förstörs av Lexbase*" (2 February 2014).

[128] Government-commissioned report (2016:58) "*Ändrade mediegrundlagar*" (September 2016).

[129] Swedish DPA opinions 1908-2016 (20 December 2016) and 413-2017 (27 February 2017).

[130] Swedish DPA newsletter "Integritet i focus" (1/2017): "*Klagomål mot appen Truecaller*" (March 2017, p. 14). Truecaller is a mobile application featuring a global telephone directory using crowdsourced data which enables it to integrate the telephone numbers registered in the list of contacts of its users. As far as we understand the contacts of the users are not necessarily aware of the processing of their personal data by Truecaller.

[131] The Swedish DPA noted in particular that, given the rules on jurisdiction set in the Data Protection Directive (Article 4) and the GDPR (Article 6), it had exclusive jurisdiction under EU law to monitor Swedish-based companies. Interestingly, the case with Truecaller, a company with over 100 million users worldwide, illustrates the risk of Sweden being used as a safe haven by certain companies in order to circumvent more restrictive data protection rules in other EU States.

Question 4.3.

According to a recent report,[132] the Nordic countries constitute a "hotbed" for the Internet of Things (IoT): "*The region is among the most mature markets in the world with almost four times as many connected devices per person than the rest of the world*". Yet, this leadership has not resulted in the adoption of IoT-specific rules.

Liability issues are dealt with under the traditional rules on e.g. product liability and tort liability as well as the contractual liability of the parties involved. An example discussed in several articles is the fictitious case of a self-driving car causing an accident as a result of sudden acceleration.[133] In such case, the chain of responsibility would have to be determined based on the role of each operator: the manufacturer of the hardware, the designer of the sensors, the software developer, the cloud provider and the local ISP.

Privacy issues are subject to the Personal Data Act. The main privacy issues related to IoT concern the lack of information of the users regarding the collection of their personal data and the risk of profiling. To our knowledge, there are no specific IoT-related cases in the Swedish courts.

However, we note that the Swedish DPA has recently been active in several cases related to the IoT. In 2015, the Authority conducted a survey of health applications.[134] The Swedish DPA identified a number of issues with some of those applications. The most serious problem concerned the authentication mechanisms which, due to the sensitive nature of the personal data collected, required more advanced tools than a simple user-ID and a PIN-code. The Authority requested in a few cases that the app developers introduce stronger authentication mechanisms such as e-IDs or one-time passwords. In other cases, the Authority called for clearer information to be provided to users on the processing of their personal data and routines for the storing of such data.

More recently, the Swedish DPA received a complaint by a consumer organisation regarding the alleged privacy breach posed by the doll "My Friend Cayla" and the intelligent robot "i-Que".[135] Similar complaints had been brought in Germany and Norway and the Swedish DPA expressed concerns that these toys were breaching safety and personal integrity rules. In particular, the DPA noted that the toys in question made it possible to spy on children, provide disguised advertising, resell personal data to third parties and were subject to terms and

[132] Arthur D. Little – TeliaSonera "Connected Things – Driving business transformation in the Nordics" (2016 edition).

[133] Dagensanalys.se "*Internet of Things och den juridiska verkligheten*" (22 March 2016) and Sofia Edvardsen "*Internet of Things – Juridisk reglering*" (1 March 2016).

[134] Swedish DPA newsletter "Integritet i fokus" (1/2015): "*Varför har ni granskat hälsoappar?*".

[135] Swedish Consumers' Association (*Sveriges Konsumenter*) "*Anmälan oskäliga avtalsvillkor*" (6 December 2016).

conditions which could change at any time. The DPA found however that it lacked jurisdiction to review the complaint as the products were manufactured in China and the USA.[136]

With regards to ownership issues, and aside from the rules on e.g. consent set in the Personal Data Act and the GDPR, the Swedish rules on copyright would apply to the production of a catalogue. Under the Copyright Act, an IoT-operator collecting data from an ecosystem would be entitled to enjoy an exclusive right to make copies of the catalogue it produces provided that it covers a large number of information items or is the result of a significant investment.[137] Note finally that Sweden is one of the few EU countries which has enacted a law protecting trade secrets.[138] The IoT operator collecting data shall in accordance with this law make sure that the data in question does not qualify as "trade secrets".

Question 4.4.

Following the ruling of the CJEU in the *Costeja* case,[139] Google has introduced routines to review complaints by individuals who wish to have search results with reference to their name de-listed. Our understanding is that Google applies similar routines in Sweden as in the other EU States.

In a recent decision, the Swedish DPA reviewed these routines and some of Google's decisions to refuse de-listing.[140]

The DPA had only a few concerns with regards to the form under which Google was handling complaints from individuals.[141] However, in line with the position of the French DPA[142] and the WP29 Guidelines,[143] the Swedish DPA argued for a "right to be forgotten" which extends beyond EU domains. In particular, the Authority found that the Swedish Personal Data Act could, under certain conditions, apply to Google' search results, even if these were provided outside Sweden. The DPA ordered therefore Google to delist search results from foreign domains

[136] Swedish DPA newsletter "Integritet i fokus" (1/2017): "*My friend Cayla-storebrors bäste vän?*" (March 2017, p. 6-8).

[137] Section 49 of the Swedish Copyright Act.

[138] Act on the Protection of Trade Secrets (1990:409) (*Lagen om skydd för företagshemligheter*).

[139] Case C-131/12 *Google Spain and Inc v. Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja González*.

[140] Swedish DPA decision in case 1013-2015 (2 May 2017). To the best of our knowledge, this decision has not been appealed before courts at the time of writing.

[141] For instance the DPA expressed some concerns that complaints may only be brought by way of a web form (as opposed to emails, faxes, etc.). Further, the DPA recommended that the information related to a de-listing which was sent to the relevant webmasters should only take place if such information did not breach the personal integrity of the plaintiff.

[142] French DPA decision dated 10 March 2016, referred to the CJEU by the French Supreme Administrative Court (pending case C-507/17 *Google*).

[143] Guidelines of the WP29 on the Implementation of the *Costeja* ruling (26 November 2014).

(such as google.com) if those results have such a "special connection" to Sweden and to the data subject that they would violate his or her personal integrity.[144]

As mentioned, the DPA also reviewed Google's decisions to refuse de-listing in 13 individual cases. In a few cases, the DPA had no comment or agreed with Google's position.[145] However, in several cases, the DPA objected to the balance struck by Google between the individual's right to data protection and the public's right to information.

In one case, the DPA agreed in principle with Google that a person who led an organisation helping child refugees played a public role and may therefore be subject to a certain level of public scrutiny. However it found that some of the information related to her private life (including her sexuality) were of no relevance for such scrutiny. In another case, the DPA found that the public's right to information did not motivate the linking to a chat forum discussing an alleged sexual abuse and the mental state of a psychiatrist.[146] As a last example, the DPA disagreed with Google that accusations of fraud related to a real estate agent and described in an old newspaper article was of such interest that it motivated a breach of his privacy rights.[147] In all those cases, the Swedish DPA ordered Google to proceed with the de-listing.

Swedish courts have also discussed the "right to be forgotten". In a recent judgment, the Svea Court of Appeal (*Svea Hovrätt*) upheld a ruling by the Stockholm District Court (*Tingsrätten*) rejecting a complaint brought by a private person against Google.[148] The case concerned the display of search results linking to news articles accusing the plaintiff of tax fraud, bankruptcy and association with organized criminality. The District Court found that the protection of privacy of the plaintiff did not outweigh the public's right to information. It referred to the fact that the plaintiff held a public role (CEO for a construction company), that he was granted a right to deny the accusations in the articles in question and that those were fairly recent (less than 5 years).

[144] As examples of a "special connection", the Swedish DPA mentions search results linking to websites in Swedish or directed to a Swedish audience.

[145] The Swedish DPA failed in those cases to see how the websites displayed on Google' search results affected the plaintiffs (e.g. the name of the plaintiffs were not mentioned or had already been deleted from these websites).

[146] The plaintiff had argued with Google that he had been acquitted from the crime of sexually abusing a patient. Note that the DPA did not question the plaintiff's version.

[147] The DPA mentioned notably that the accusations had not been proven and related to facts having taken place more than 10 years ago.

[148] Svea Court of Appeal in case T-4721-16 (5 May 2017) and Stockholm District Court in case T-4355-15 (9 May 2016).

SWITZERLAND

Jacques Beglinger

Einleitung: Die Schweiz und der (digitale) EU-Binnenmarkt

Im Jahr 2015 präsentierte die Europäische Kommission ihre „Strategie für einen digitalen Binnenmarkt in Europa" und führte dazu aus: „In einem digitalen Binnenmarkt ist der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleistet und können Privatpersonen und Unternehmen unter fairen Wettbewerbsbedingungen und auf der Grundlage hoher Verbraucher- und Datenschutzstandards ungeachtet ihrer Staatsangehörigkeit bzw. ihres Wohn- oder Geschäftssitzes nahtlos Online-Aktivitäten nachgehen und Internetanwendungen nutzen. Mit der Vollendung des digitalen Binnenmarkts wird gewährleistet, dass Europa auch in Zukunft zu den Vorreitern der Digitalwirtschaft gehört und den europäischen Unternehmen zur Expansion auf den Weltmärkten verhelfen kann."[1]

Sowohl im Titel als auch im zitierten Text ist von „*Europa*" die Rede. Allerdings bestehen heute umfassende Regelungen für den im Text angesprochenen freien Verkehr von Waren, Personen, Dienstleistungen und Kapital nur in zwei geographischen Dimensionen, nämlich einerseits innerhalb der EU (Art. 3 Abs. 3 EUV, Art. 26 ff. AEUV) und andererseits zwischen der EU und den drei EWR/EFTA-Staaten Island, Liechtenstein und Norwegen (Art. 1 Abs. 2 sowie Art. 8 ff. EWR-Abkommen). Dementsprechend ist auch die mit dem digitalen Binnenmarkt verbundene EU-Gesetzgebung in diesen beiden Dimensionen relevant.

[1] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 final.

So begrüsst z.B. der Gemischte Parlamentarische Ausschuss des EWR die digitale Binnenmarktstrategie der EU-Kommission ausdrücklich und weist in einer Resolution darauf hin, dass das EWR-Abkommen „provides for the EEA EFTA States' participation in the Internal Market of the European Union in various fields related to the Digital Single Market Strategy".[2]

Im Vergleich dazu nimmt die *Schweiz in ihrem europäischen Umfeld eine besondere Stellung* ein: Sie ist zwar der vierte EFTA-Staat, gehört aber nicht zum EWR. Der EWR-Beitritt wurde anfangs der 1990er Jahre von der Schweizerischen Bundesregierung angestrebt und die Schweiz war damals massgeblich an den Verhandlungen über das EWR-Abkommen beteiligt. Allerdings scheiterte der Beitritt Ende 1992 an einer negativen Volksabstimmung.[3] Stattdessen setzte die Schweiz in ihrem Verhältnis zu den damaligen Europäischen Gemeinschaften den bereits in den 1950er Jahren eingeschlagenen Weg fort und schloss mit ihnen bzw. später mit der EU für spezifische Bereiche sog. bilaterale (schweizerische Terminologie) bzw. sektorielle (EU-Terminologie) Abkommen.[4] Einige dieser Abkommen umfassen ausgewählte Aspekte des Waren-, Personen- und Dienstleistungsverkehrs und werden deshalb als „Marktzugangsabkommen" bezeichnet. Diese Abkommen führen aber im Unterschied zum EWR *nicht zu einer umfassenden Assoziation der Schweiz mit dem EU-Binnenmarkt*.[5] Dies betont auch der Gerichtshof der Europäischen Union in einer das Verhältnis zwischen der Schweiz und der EU betreffenden Entscheidung nachdrücklich, wenn er Folgendes ausführt:[6]

[2] EEA Joint Parliamentary Committee, Resolution on the Digital Single Market Strategy, 19 November 2015, Punkt J in der Präambel, http://www.europarl.europa.eu/cmsdata/96084/45th%20EEA%20JPC%20Resolution%20on%20the%20Digital%20Single%20Market%20Strategy.pdf (zuletzt besucht: 30.9.2017).

[3] Philippe G. Nell, *Suisse-Communauté Européenne. Au coeur des négotiations sur l'Espace économique européen*, Paris: Economica 2012; Sicht Dieter Freiburghaus, *Königsweg oder Sackgasse? Schweizer Europapolitik von 1945 bis heute*, 2. überarbeitete Auflage, Zürich: Verlag Neue Zürcher Zeitung 2015.

[4] Zum Ganzen siehe etwa Thomas Cottier et al., *Die Rechtsbeziehungen der Schweiz und der Europäischen Union*, Bern: Stämpfli 2014; Christa Tobler/Jacques Beglinger, *Grundzüge des bilateralen (Wirtschafts-) Rechts. Systematische Darstellung in Text und Tafeln*, 2 Bände (Text und Tafeln), Zürich/St. Gallen: Dike 2013.

[5] Dazu Christa Tobler, Jeroen Hardenbol & Ballász Mellár (für das Europäische Parlament), *Internal Market Beyond the EU: EEA and Switzerland*, Strasbourg/Brussels: European Parliament 2010; Christa Tobler/Georges S. Baur, ‚Der Binnenmarkt ist (k)ein Schweizer Käse. Zum Assoziationsstatus der Türkei, der EWR/EFTA-Staaten und der Schweiz, insb. mit Bezug auf den EU-Binnenmarkt', in: Astrid Epiney, Markus Kern & Lena Hehemann (Hrsg.), *Schweizerisches Jahrbuch für Europarecht 2014/2015*, Bern: Stämpfli & Zürich/Basel/Genf: Schulthess 2015, 331-345.

[6] EuGH, Rs. C-547/10 P *Schweizerische Eidgenossenschaft gegen Kommission*, ECLI:EU:C:2013:139, Erw. 78 f. Zu dieser Entscheidung äusserten sich in der Schweiz etwa Laura Melusine Baudenbacher, ‚EuGH überträgt die Polydor-Rechtsprechung auch auf das Luftverkehrsabkommen', *European Law Reporter* 2013, 173-182, sowie Christa Tobler, ‚Luftverkehrsrecht: Auslegung des Luftverkehrsabkommens EU-

„[...] ist darauf hinzuweisen, dass das Luftverkehrsabkommen EG–Schweiz zu einer Reihe von sieben sektorbezogenen Abkommen zwischen denselben Vertragsparteien gehört, die am 21. Juni 1999 unterzeichnet wurden, mithin nach der am 6. Dezember 1992 erfolgten Zurückweisung des Abkommens über den Europäischen Wirtschaftsraum vom 2. Mai 1992 (ABl. 1994, L 1, S. 3) durch die Schweizerische Eidgenossenschaft, mit der diese das Vorhaben eines integrierten wirtschaftlichen Ganzen mit einem einheitlichen Markt, gestützt auf gemeinsame Regeln für seine Mitglieder, abgelehnt und es vorgezogen hat, in bestimmten Bereichen bilaterale Vereinbarungen mit der Europäischen Union und ihren Mitgliedstaaten abzuschließen [...]. Daher ist die Schweizerische Eidgenossenschaft nicht dem Binnenmarkt der Union beigetreten, mit dem alle Hindernisse beseitigt werden sollen, um einen Raum vollständiger Freizügigkeit entsprechend einem nationalen Markt zu schaffen [...]."

Diese Sachlage hat *Folgen für die vorliegend zu behandelnde Thematik*: So ist die in der Fragestellung erwähnte Sekundärgesetzgebung der EU zwar durchgehend für den EWR relevant, nicht aber in gleichem Masse für die Schweiz und die bilateralen bzw. sektoriellen Abkommen. Dies liegt v.a. daran, dass die für das vorliegende Thema relevante EU-Sekundärgesetzgebung thematisch hauptsächlich zum Bereich der Dienstleistungen und des Verbraucherschutzes gehört. Letzteres wird aber vom bilateralen bzw. sektoriellen Recht zwischen der Schweiz und der EU praktisch gar nicht und Ersteres nur eingeschränkt erfasst. Insbes. besteht zwischen diesen Parteien kein umfassendes Dienstleistungsabkommen. Neben den sektorspezifischen Abkommen über den Land-[7] und den Luftverkehr[8] enthält das Freizügigkeitsabkommen[9] einige, im Vergleich zum EU- und dem EWR-Recht allerdings eingeschränkte, allgemeine Bestimmungen über die Dienstleistungsfreiheit. Hierzu gehört aber nur sehr wenig EU-Sekundärrecht, zu dem die für die vorliegende Thematik relevante Gesetzgebung gerade nicht gehört. Tatsächlich ergeben sich im Rahmen der vorliegenden Thematik *für die Schweiz nur gerade im Bereich des Datenschutzes unmittelbare rechtliche Berüh-*

Schweiz – Keine Anwendbarkeit der Dienstleistungsfreiheit', *Europäische Zeitschrift für Wirtschaftsrecht* 2013, 432-434.

[7] Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Güter- und Personenverkehr auf Schiene und Strasse, für die Schweiz SR 0.740.72, für die EG (heute die EU) ABl. 2002 L 114/91.

[8] Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Luftverkehr, für die Schweiz SR 0.748.127.192.68, für die EG (heute die EU) ABl. 2002 L 114/73.

[9] Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft einerseits und der Europäischen Gemeinschaft und ihren Mitgliedstaaten andererseits über die Freizügigkeit, für die Schweiz SR 0.142.112.681, für die EG (heute die EU) und ihre Mitgliedstaaten ABl. 2002 L 114/6.

rungspunkte, weil diese Thematik von den Schengen-[10] und Dublin-Assoziationsabkommen[11] zwischen der Schweiz und der EU erfasst wird.

Dies heisst nun allerdings nicht, dass das EU-Recht aus der Sicht der Schweiz überall dort irrelevant ist, wo zu einer bestimmten Thematik kein Abkommen vorliegt. Vielmehr verfolgt die Schweiz insbesondere seit dem oben erwähnten Referendum über die EWR-Mitgliedschaft neben dem „bilateralen Weg" zusätzlich den Weg des sog. *autonomen Nachvollzugs*.[12] Dabei handelt es sich um eine einseitige Strategie, vermittels welcher die Schweiz ihr nationales Recht dem EU-Recht anpasst, um auf diese Weise den Wirtschaftsaustausch auch in Bereichen ausserhalb von Abkommen zu erleichtern. Je nach dem Bereich erfolgt dies auch im Hinblick auf eine *Äquivalenzentscheidung (Angemessenheitsbschluss) der EU*, die in der EU-internen Regelgebung für Drittstaaten vorgesehen ist. Auch diese Thematik ist im schweizerischen Datenschutz in besonderer Weise relevant.

Vor diesem Hintergrund und angesichts der *europarechtlichen Orientierung der hier zu behandelnden Thematik* erscheint es daher sinnvoll, dass der *vorliegende Bericht über die Schweiz auf den Fragebereich „4. Daten in der digitalen Wirtschaft" fokussiert*.

Zu den *übrigen Themen* sei an dieser Stelle darauf hingewiesen, dass sich in diversen Schweizer Materalien zur Digitalisierung häufig fundierte Informationen und Einschätzungen zu den Fragebereichen „1. Binnenmarkt und elektronischer Kommerz: Internet und E-Kommerz", „2. Digitale Media" und „3. Digitale Infrastrukturen" finden, allerdings überwiegend mit Bezug auf die politischen, gesellschaftlichen und wirtschaftlichen (statt der rechtlichen) Rahmenbedingungen.

So befassen sich verschiedene *Publikationen der Schweizer Bundesregierung (Bundesrat)* intensiv mit den Rahmenbedingungen der Digitalisierung in der Schweiz und der Positionierung der Schweiz gegenüber der Digitalisierung im EU-Raum. Dazu gehören namentlich:

[10] Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, für die Schweiz SR 0.362.31, für die EU und die EG (heute nur noch die EU) ABl. 2008 L 53/52.

[11] Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags, für die Schweiz SR 0.142.392.68, für die EG (heute die EU) ABl. 2008 L 53/5.

[12] Hierzu etwa Walter A. Stoffel/Claudia Seitz, ‚Autonomer Nachvollzug – Das Wirtschaftsrecht der Schweiz zwischen Angleichung und Eigenständigkeit', *Europäische Zeitschrift für Wirtschaftsrecht* 2012, 841-843.

• *Strategie „Digitale Schweiz"*[13] vom 24.4.2016, wo u.a. die digitale Wirtschaft,[14] die digitalen Infrastrukturen[15] und neue Formen der politischen Partizipation einschliesslich der digitalen Medien[16] als Aktionsfelder genannt sind. Die Strategie „Digitale Schweiz" wird ergänzt durch den *Bericht 2012-2015 zur Umsetzung der Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz vom März 2012*,[17] ebenfalls vom 24.4.2016, erstellt vom Bundesamt für Kommunikation.[18]

In Bezug auf die EU-Strategie für einen digitalen Binnenmarkt soll angestrebt werden, „den Dialog mit der EU zu führen, die Aktivitäten auf Schweizer Seite zu koordinieren und so die Chancen, die der digitale Binnenmarkt mit sich bringt, auch für die Schweiz nutzbar zu machen und das Risiko einer Ausgrenzung abzuwenden."[19] In der Umsetzung wird dieser Aspekt als prioritär erklärt.[20]

• *Bundesrätlicher Bericht „Rahmenbedingungen der digitalen Wirtschaft"*, erstellt vom Staatssekretariat für Wirtschaft (SECO), vom 11.1.2017,[21] inkl. Ausführungen zu den Themen Geoblocking und kollaborative Wirtschaft.[22] Mit gleichem Datum erteilte der Bundesrat zudem weitere Prüfungsaufträge:[23]

[13] Schweizerische Eidgenossenschaft, Bundesamt für Kommunikation, Strategie „Digitale Schweiz", BBl 2016 3985, https://www.bakom.admin.ch/dam/bakom/de/dokumente/informationsgesellschaft/strategie/strategie_digitale_schweiz.pdf.download.pdf/strategie_digitale_schweiz_DE_Barrierefrei.pdf (zuletzt besucht: 30.9.2017). Siehe dazu auch die zusammenfassende Broschüre „Strategie Digitale Strategie", April 2016, https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/digitale_schweiz_und_internet/Strategie%20Digitale%20Schweiz/Strategie/Strategie%20Digitale%20Schweiz.pdf.download.pdf/strategie_digitale_schweiz_Brosch%C3%BCre.pdf (zuletzt besucht: 30.9.2017).

[14] Idem, 4.1. Digitale Wirtschaft, S. 6.

[15] Idem, 4.3. Infrastrukturen und Umwelt, S. 6.

[16] Idem, 4.5. Neue Formen der politischen Partizipation, S. 9.

[17] Bundesamt für Kommunikation, Bericht 2012-2015 zur Umsetzung der Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz vom März 2012, April 2016, https://www.bakom.admin.ch/infosociety (zuletzt besucht: 30.9.2017).

[18] Medienmitteilung vom 20.4.2016: Strategie des Bundesrates für eine digitale Schweiz, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-61417.html (zuletzt besucht: 30.9.2017).

[19] Strategie „Digitale Schweiz" (Fn. 13), S. 13.

[20] Aktionsplan Strategie "Digitale Schweiz", Massnahmen der Bundesverwaltung, 20.4.2016, S. 7, https://www.bakom.admin.ch/dam/bakom/de/dokumente/informationsgesellschaft/strategie/aktionsplan_digitale_schweiz.pdf.download.pdf/aktionsplan_digitale_schweiz_DE.pdf (zuletzt besucht: 30.9.2017), sowie die Umsetzungsplanung des Bundesrats, https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz/aktionsplan.html (zuletzt besucht: 30.9.2017).

[21] Schweizerische Eidgenossenschaft, Staatssekretariat für Wirtschaft (SECO), Bericht über die zentralen Rahmenbedingungen für die digitale Wirtschaft, Bericht des Bundesrats vom 11. Januar 2017, https://www.newsd.admin.ch/newsd/message/attachments/46892.pdf (zuletzt besucht: 30.9.2017).

[22] Idem, Wettbewerbspolitik, S. 159 ff.; Geoblocking, S. 169 ff., sowie Sharing Economy, S. 95 ff.

[23] Medienmitteilung vom 11.1.2017: Bundesrat verabschiedet Bericht zu Rahmenbedingungen der digitalen Wirtschaft, https://www.seco.admin.ch/seco/de/home/seco/nsb-news/medienmitteilungen-2017.msg-id-65223.html (zuletzt besucht: 30.9.2017).

„Der Bundesrat beschloss, in verschiedenen Bereichen Massnahmen zu prüfen beziehungsweise die Entwicklung zu verfolgen:

1. Beherbergungsplattformen: Bis Ende 2017 werden Unschärfen im Mietrecht bezüglich den Zustimmungsmodalitäten des Vermieters zur Untermiete geklärt.

2. Multimodale Dienstleistungen: Dem Bundesrat wird bis Ende 2017 dargelegt, wie private und öffentliche Mobilitätsdienstleistungen besser vernetzt werden können.

3. Wettbewerbspolitik: Ebenfalls bis Ende 2017 wird abgeklärt, ob Fusionen von Internet-Plattformen mit geringen Umsätzen von den Behörden geprüft werden können, indem die Aufgreifschwelle angepasst wird.

4. „Digitaler Test": Gestützt auf Umfragen bei den betroffenen Verbänden und Sozialpartnern wird dem Bundesrat bis Ende 2018 aufgezeigt, welche Gesetzesartikel die Digitalisierung behindern.

5. Bildungs- und Forschungspolitik: Unter Einbezug der Kantone und der Hochschulkonferenz ist bis Ende Juni 2017 zu prüfen, welche Auswirkungen die Digitalisierung auf den Bildungs- und Forschungsbereich hat und ob Massnahmen notwendig sind.

6. Internationale Regulierung: Die internationalen Entwicklungen der wirtschaftspolitischen Regulierungen der Digitalen Wirtschaft sind zu verfolgen und bis Ende 2018 ist allfälliger Handlungsbedarf aufzuzeigen."

- Im Hinblick auf die Beurteilung der Anforderungen an die digitale Infrastruktur (namentlich Identität- und Zugangsmanagement) im europäischen Umfeld beauftragte das SECO zudem das E-Government-Institut der Fachhochschule Bern, „die Umsetzung der Strategie für einen digitalen Binnenmarkt in Europa (Digital Single Market, DSM) zu beobachten und daraus Implikationen für die weitere Entwicklung der digitalen Infrastruktur in der Schweiz herauszuarbeiten". Die Resultate sollen das SECO bei den Arbeiten an den Infrastrukturen im Bereich Identitäts- und Access Management (IAM) unterstützen. Ein entsprechender gemeinsamer Zwischenbericht wurde im Februar 2017 veröffentlicht.[24]
- Zwischenanalyse *Die Schweiz und der digitale Binnenmarkt der EU* vom 7.6.2017,[25] erstellt von den federführenden Departementen im Rahmen der Umsetzung der Strategie „Digitale Schweiz".

[24] Staatssekretariat für Wirtschaft (SECO) & Berner Fachhochschule, Digital Single Market-Infrastruktur- Observatorium – Anschlussfähigkeit der Schweiz an die europäischen digitalen Infrastrukturen, Projektzwischenbericht, Version 1.1, Februar 2017, https://www.wirtschaft.bfh.ch/uploads/tx_frppublikationen/Zwischenbericht_Digital_Single_Market.pdf (zuletzt besucht: 30.9.2017).

[25] Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK), Eidgenössisches Departement für auswärtige Angelegenheiten (EDA), Eidgenössisches Finanzdepartement (EFD) und Eidgenössisches Department für Wirtschaft, Bildung und Forschung (WBF), Die Schweiz und der digitale Binnenmarkt der EU, Stand: 07. Juni 2017, https://www.bakom.admin.ch/dam/bakom/de/dokumente/informationsgesellschaft/mise%20en%20oeuvre/DSM_EU-

In diesem Bericht werden die Zielsetzungen jeder einzelnen der 16 Massnahmen der EU-Strategie für einen digitalen Binnenmarkt (DSM-Strategie) sowie die aktuelle Situation in der Schweiz vorgestellt, zusammen mit einer aktuellen Einschätzung zum allfälligen Handlungsbedarf für den Bund durch die jeweils thematisch zuständigen Bundestellen. Die neuen Vorschläge der EU-Kommission vom 10.5.2017 im Zusammenhang mit ihrer Halbzeitbewertung der DSM-Strategie[26] sind in die Analyse einbezogen.

Unternehmensseitig hat insbesondere der Dachverband der Schweizer Wirtschaft, economiesuisse, am 22.8.2017 die breite Studie *Zukunft digitale Schweiz* veröffentlicht und damit ebenfalls eine umfassende Einschätzung der wirtschaftlichen Prioritäten in nationaler und internationaler Hinsicht vorgelegt.[27]

1.3. Binnenmarkt und elektronischer Kommerz: Internet und E-Kommerz, Digitale Media, Digitale Infrastrukturen

[Aufgrund der besonderen europarechtlichen Situation der Schweiz nicht behandelt.][28]

4. Daten in der digitalen Wirtschaft

4.1. Vorbereitungen auf das Inkrafttreten des DSGVO

Die Beantwortung dieser Frage mit Bezug auf die Schweiz erfordert gewisse Hintergrundinformationen. Im Folgenden wird daher vorab die Frage angesprochen, inwiefern die EU-Verordnung 2016/679[29] (Datenschutzgrundverordnung, DSGVO) für die Schweiz als Drittstaat überhaupt verbindlich ist. Anschliessend wird vor diesem Hintergrund auf die in der Schweiz laufende Revision des Datenschutzrechts eingegangen. Ein weiterer, ergänzender Teil betrifft den Schutz der Privatsphäre in der elektronischen Kommunikation.

CH.pdf.download.pdf/DSM%20UE%20et%20cons%C3%A9quences%20pour%20la%20CH_DE.pdf (zuletzt besucht: 30.9.2017).

[26] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt Ein vernetzter digitaler Binnenmarkt für alle, COM(2017) final. Siehe auch Pressemitteilung, Digitaler Binnenmarkt: Kommission ruft zur zügigen Annahme der wichtigsten Vorschläge auf und präzisiert die anstehenden Herausforderungen, 10.5.2017, http://europa.eu/rapid/press-release_IP-17-1232_de.htm (zuletzt besucht: 30.9.2017).

[27] economieuisse, Zukunft digitale Schweiz, Wandel gemeinsam gestalten, Zürich 22.8.2017, https://www.economiesuisse.ch/de/artikel/zukunft-digitale-schweiz-den-wandel-gemeinsam-gestalten (zuletzt besucht: 30.9.2017).

[28] Siehe dazu aber die oben erwähnten Hinweise in den diversen offiziellen Dokumenten sowie insbes. der Bericht „Die Schweiz und der digitale Binnenmarkt der EU" (Fn. 25).

[29] Verordnung 2016/679/EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119/8.

Ist die DSGVO für die Schweiz verbindlich?

Durch die Schengen- und Dublin-Assoziationen der Schweiz mit der EU haben u.a. *datenschutzrechtliche Regelungen Eingang in das schweizerische Recht gefunden, die dem EU-Recht entstammen*.[30] Zur Zeit (Ende September 2017) handelt es sich noch um die Richtlinie 95/46,[31] ergänzt durch den Rahmenbeschluss 2008/977.[32] Beide werden im Rahmen der Revision des EU-Datenschutzrechts durch neuere Rechtsakte ersetzt, u.a. durch die bereits erwähnte Datenschutz-Grundverordnung 2016/679 und die Richtlinie 2016/680.[33] Während beide Rechtsakte klarerweise für den EWR-relevant sind,[34] liegen die Dinge mit Bezug auf die Schweiz komplexer.

Unbestritten ist, dass die Richtlinie 2016/680 Teil des Assoziations-Acquis der Schweiz werden soll.[35] Anders die hier interessierende DSGVO: Obwohl sie die zum bilateralrechtlichen Acquis gehörende Richtlinie 95/46 ersetzt, ist sie von der EU letztlich nicht als bilateralrechtlich eingestuft worden. Zwar hatte sich die Schweiz für die Assoziationsrelevanz der neuen Verordnung ausgesprochen und schlug die Kommission dies auch vor. Im Gesetzgebungsverfahrens strich aber der Rat dieses Element wieder aus der Vorlage.[36] In der Folge wurde die DSGVO weder als bilateralrechtlich relevant gekennzeichnet noch der Schweiz als solche notifiziert. Die Schweizer Bundesverwaltung (Bundesamt für Justiz, BJ) geht angesichts dieser Sachlage davon aus, dass die DSGVO für die Schweiz nicht assoziationsrelevant ist, sondern vielmehr ausschliesslich im Rahmen von Äquivalenzüberlegungen zu beachten ist (Weiteres dazu in den folgenden Abschnitten).

[30] Hierzu Luzius Mader/Martin Hilti, ‚Europarechtliche Vorgaben im Bereich Datenschutz: Implikationen', in: Astrid Epiney/Tobias Fasnacht (Hrsg.), *Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes und Implikationen für die Schweiz*, Zürich/Basel/Genf: Schulthess 2012, 69-86.

[31] Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, 1995 ABl. L 281/31.

[32] Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. 2008 L 350/60.

[33] Richtlinie 2016/680/EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. 2016 L 119/89.

[34] Im EWR-Kontext war anfangs umstritten, ob die DSGVO zum EWR-Acquis oder zum (von den EWR/EFTA-Staaten mit der EU separat geregelten) Schengen-Acquis gehört. Dazu Georges Baur, ‚Datenschutz-Grundverordnung Schengen-relevant? Vielleicht nicht, aber …', in: *Schengen in der Praxis* (2017), im Erscheinen begriffen.

[35] Dazu Christa Tobler, 'Homogenität im Rechtsbestand der Schengen- und Dublin-Abkommen: Übernimmt die Schweiz im Assoziationsrahmen nicht notifiziertes Asyl- und Datenschutzrecht der EU?', *Swiss Review of International and European Law* 27 (2017), 211-226, S. 221 f.

[36] Laut Tobler (Fn. 35), S.221, erfolgte dies möglicherweise, um so eine potentielle Sonderstellung des Vereinigten Königreichs und Irlands auszuschliessen.

Im schweizerischen wissenschaftlichen Schrifttum ist die Frage umstritten. So ist Epiney der Auffassung, dass „zwar grundsätzlich ein Einbezug von Weiterentwicklungen des EU-Sekundärrechts im Rahmen der Schengen/Dublin- Assoziierung nur insoweit in Betracht kommt, wie das im Abkommen vorgesehene Übernahmeverfahren durchlaufen wurde, hiervon jedoch dann eine Ausnahme anzunehmen ist, wenn ein Rechtsakt klar und eindeutig als Weiterentwicklung des Schengen/Dublin-Besitzstands anzusehen ist, eine Notifizierung jedoch gleichwohl unterblieben ist und daher die Parallelität der Rechtsentwicklung in Frage gestellt wird".[37] Die Autorin stützt damit letztlich die Auffassung des Eidgenössischen Datenschutzbeauftragten (EDÖB),[38] der die DSGVO auch ohne formelle Übernahme durch die Schweiz als anwendbar erachten will.[39] Umgekehrt teilt Tobler[40] die Auffassung des Schweizer Bundesamtes für Justiz (BJ) und geht davon aus, dass im Verhältnis Schweiz-EU statt der DSGVO weiterhin die Richtlinie 45/96 anwendbar ist. Die folgenden Ausführungen gehen vom letzteren Szenario aus, da sich die Revisionstätigkeit der Bundesverwaltung mit Bezug auf den Datenschutz hier situiert.

Revision des Schweizer Datenschutzrechts

Die Schweiz ist dem Europaratsübereinkommen No. 108[41] beigetreten. Das *Übereinkommen stellt das europarechtliche Fundament des Schweizer Datenschutzrechts dar.* Die in der Schweiz zur Zeit laufende Modernisierung des nationalen Datenschutzgesetzes soll u.a. die ebenfalls laufende Revision des Übereinkommens berücksichtigen. Weiter strebt die Bundesverwaltung eine *Annäherung an die Anforderungen der DSGVO* der EU an. Das Bundesamt für Justiz führt hierzu aus: „Diese Annäherung und die Ratifizierung des revidierten Übereinkommens [...] 108 sind zentral, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt und die grenzüberschreitende Datenübermittlung auch künftig möglich bleibt."[42]

[37] Astrid Epiney, ‚Verweise auf EU-Sekundärrecht im Bilateralen Recht. Zur Reichweite von Verweisen auf EU-Sekundärrecht in den Bilateralen Abkommen bei der Weiterentwicklung des Unionsrechts', *Jusletter* 11. September 2017, Rz. 33.

[38] Webpräsenz des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB): https://www.edoeb.admin.ch (zuletzt besucht: 30.9.2017).

[39] Dazu Tobler (Fn. 35), S.223.

[40] Idem, S. 223 ff.

[41] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 [ETS 108], für die Schweiz in Kraft seit 1. Februar 1998, SR 0.235.1. Im Jahr 2007 ratifizierte die Schweiz ausserdem das Zusatzprotokoll bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 8. November 2001, SR 0.235.11.

[42] Schweizerische Eidgenossenschaft, Bundesamt für Justiz, Stärkung des Datenschutzes, https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html (zuletzt besucht: 30.9.2017).

Dabei geht es um die bereits am Anfang dieses Berichts erwähnte *Äquivalenz bzw. die Angemessenheit* nach den Bestimmungen der DSGVO, wobei der Standard des Europaratsübereinkommens No. 108 ein wesentliches Element darstellt (Erw. 105 in der Präambel der DSGVO).[43] Tobler[44] bemerkt hierzu: „Mit der Äquivalenzerklärung bringt die EU zum Ausdruck, dass sie das betreffende Land mit Blick auf Datenschutzbelange sozusagen als « sicheren Drittstaat » einstuft, dem sie vertrauen kann. Im Rahmen des bisherigen EU-Rechts liegt für die Schweiz eine Äquivalenzentscheidung der Europäischen Kommission vor, die allerdings je nach der künftigen Entwicklung auch wieder aufgehoben werden könnte." Die heute für die Schweiz geltende Äquivalenzerklärung bzw. der Angemessenheitsbeschluss der EU-Kommission stammt aus dem Jahr 2000 und bezieht sich auf die Richtlinie 95/46.[45] Hier stellen die Annahme der DSGVO der EU sowie die laufende Revision des Europaratsübereinkommens No. 108 für die Schweiz Herausforderungen dar, welche massgeblich zur nun laufenden Revision des nationalen Datenschutzrechtes geführt haben (dazu auch im nachfolgenden Abschnitt).

Was nun die DSGVO anbelangt, auf welche sich die Frage 4.1. bezieht, so gilt es nochmals festzuhalten, dass die Revisionsarbeiten in der Schweiz mit Blick auf die Frage der Äquivalenz erfolgen, und damit in einem rechtlich anderen Rahmen als im Falle der EU-Mitgliedstaaten und – im Zuge der Übernahme in das EWR-Recht – der EWR/EFTA-Staaten. Vor diesem Hintergrund sind in der Schweiz bis jetzt (Ende September 2017) die folgenden gesetzgeberischen Schritte zu verzeichnen:

- Am 19.10.2014 legte die Begleitgruppe Revision DSG ihren Bericht „Normkonzept zur Revision des Datenschutzgesetzes" vor.[46]
- Am 21.12.2016 schickte der Bundesrat (Schweizer Bundesregierung) seinen Vorentwurf zu einer Totalrevision des Datenschutzgesetzes (VE-DSG) in die sog. Vernehmlassung, also in die öffentliche Konsultation.[47]

[43] Siehe hierzu wie auch umgekehrt zu den Äquivalenzbestimmungen im Schweizer Recht Monique Cossali Sauvain, ‚Protection des donnée et flux transfrontières. Tour d'horizon du cadre législatif européen et suisse', in: Astrid Epiney/Lena Hehemann (Hrsg.), *Schweizerisches Jahrbuch für Europarecht 2015/2016*, Berne: Stämpfli / Zurich/Basel/Geneva: Schulthess 2017, 343-355, S. 350 ff.

[44] Tobler (Fn. 35), S.220.

[45] Entscheidung 2000/518/EU gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz, ABl. 2000, L 215/1.

[46] Normkonzept zur Revision des Datenschutzgesetzes. Bericht der Begleitgruppe Revision DSG, https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-d.pdf (zuletzt besucht: 30.9.2017).

[47] Medienmitteilung des Bundesrats vom 21.12.2016: Mehr Transparenz und stärkere Kontrolle über die eigenen Daten, https://www.bj.admin.ch/bj/de/home/aktuell/news/2016/ref_2016-12-21.html (zuletzt

Letztere zeigte in der Mehrheit ein Interesse an der Beibehaltung der Äquivalenz mit dem Datenschutzrecht der EU.[48]

- Am 15.9.2017 verabschiedete der Bundesrat[49] einen Entwurf zur „Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz“[50] sowie einen erläuternden Bericht hierzu, die sogenannte Botschaft.[51]

Einfluss des Europarechts auf die Schweizer Revision

Die soeben erwähnte Botschaft äussert sich u.a. zum international- und europarechtlichen Kontext der Revision des Schweizer Datenschutzrechts. Was die *Vorgaben des Europarats* betrifft, so beruht der nun vorliegende Schweizer Entwurf auf dem Entwurf zur Revision des Europaratsübereinkommens No. 108[52] in der Fassung vom September 2016.[53]

Zum *EU-Datenschutzrecht* schreibt der Bundesrat:[54]

> „Für die Schweiz ist die Richtlinie (EU) 2016/680 Bestandteil des Schengen--Acquis. Aufgrund des Schengen-Assoziierungsabkommens muss die Schweiz die Richtlinie umsetzen. Hingegen ist sie nicht verpflichtet, die Verordnung (EU) 2016/679 zu übernehmen, da es sich gemäss der Europäischen Union dabei nicht um eine Weiterentwicklung des Schengen-Acquis handelt.“

besucht: 30.9.2017), mit Links zu den relevanten Dokumenten.

[48] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, S. 4, u.a. S. 25 f. https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/bot-d.pdf (zuletzt besucht: 30.9.2017). Siehe zur Konsultation insgesamt auch Bundesamt für Justiz, Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens, 10.8.2017, https://www.admin.ch/ch/d/gg/pc/documents/2826/Totalrevision-des-Datenschutzgesetzes_Ergebnisbericht_de.pdf (zuletzt besucht: 30.9.2017), sowie.

[49] Medienmitteilung des Bundesrats: Den Datenschutz verbessern und den Wirtschaftsstandort stärken, 15.9.2017, https://www.bj.admin.ch/bj/de/home/aktuell/news/2017/ref_2017-09-150.html (zuletzt besucht: 30.9.2017).

[50] Entwurf Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, 15.9.2017, https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/entw-d.pdf (zuletzt besucht: 30.9.2017).

[51] Botschaft (Fn. 48). Die Botschaft des Schweizer Systems entspricht der Begründung, welche die Kommission im EU-Recht ihren Vorschlägen für neues Sekundärrecht voranstellt.

[52] Europarat, CAHDATA, Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data [ETS No. 108], September 2016, https://rm.coe.int/16806a616c (zuletzt besucht: 30.9.2017).

[53] Botschaft (Fn. 48), S. 27.

[54] Idem, S. 25.

Vor diesem Hintergrund legte der Bundesrat am 15. September 2017 ebenfalls den Entwurf eines Bundesbeschlusses betr. die Übernahme der EU-Richtlinie 2016/680 in den bilateralrechtlichen Schengen-Acquis vor.[55]

Im Übrigen schreibt der Bundesrat Folgendes zur Äquivalenz der Rechtsordnungen:[56]

> „In den Bereichen, die nicht der Schengen-Zusammenarbeit unterstehen, gilt die Schweiz als Drittstaat. Zwischen einem Drittstaat und den Mitgliedstaaten der Europäischen Union dürfen Daten nur ausgetauscht werden, wenn der Drittstaat ein angemessenes Schutzniveau gemäss der Richtlinie 95/46/EG gewährleistet. Dieses Schutzniveau wird durch die Europäische Kommission periodisch überprüft und in einem Angemessenheitsbeschluss festgehalten. Ein solcher Beschluss kann jederzeit widerrufen werden. [...]
>
> Mit Schreiben vom 25. Januar 2017 hat die Europäische Kommission die Mission der Schweiz bei der Europäischen Union nach einem Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015 (Rechtssache «Schrems») darüber informiert, dass sie das von den Drittländern mit einem Angemessenheitsbeschluss gewährleistete angemessene Datenschutzniveau regelmässig überprüfen muss. Die Europäische Kommission hat die Schweiz deshalb darum ersucht, ihr einen Bericht zukommen zu lassen, in dem die rechtliche Ausgangslage im Bereich Datenschutz sowie die hauptsächlichen Gesetzesänderungen seit 2000 dargelegt werden. Der Bericht wird der Europäischen Kommission vor Ende 2017 übermittelt werden.
>
> Künftig wird die schweizerische Gesetzgebung anhand der in der Verordnung (EU) 2016/679 enthaltenen Anforderungen überprüft. Falls die Schweiz den Angemessenheitsbeschluss beibehalten bzw. im Falle eines Widerrufs erneut eine Bestätigung über das angemessene Datenschutzniveau erhalten möchte, ist es insbesondere für die Wirtschaft von zentraler Bedeutung, dass die schweizerische Gesetzgebung einen den Anforderungen dieser Verordnung entsprechenden Schutz gewährleistet."

Abzuwarten bleibt, ob allfällige Nachfolgerechtsprechung des EuGH[57] auch hier Folgen haben wird.

[55] Bundesbeschluss: Entwurf über die Genehmigung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (Weiterentwicklung des Schengen-Besitzstands), https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/entw-bbl-d.pdf (zuletzt besucht: 30.9.2017).

[56] Botschaft (Fn. 48), S. 25 f.

[57] Zu erwarten ist offenbar ein Vorabentscheidungsersuchen aus Irland; vgl. dazu https://euobserver.com/justice/139264?utm_medium=rss (zuletzt besucht: 4.10.2017).

Ergänzend: Schutz der Privatsphäre in der elektronischen Kommunikation
Keinen eigenständigen Niederschlag hat der von der EU-Kommission im Januar 2017 vorgelegten Entwurf für eine Verordnung über den Schutz der Privatsphäre in der elektronischen Kommunikation[58] gefunden. Der Verordnungsvorschlag ist noch weit von einer Bereinigung entfernt. Es ist deshalb schwierig, mögliche Konsequenzen abzuschätzen oder derzeit zu entscheiden, ob eine Berücksichtigung in der Schweizer Gesetzgebung sinnvoll sein wird.[59] Dabei würde es sich aus der Sicht der Schweiz um eine autonome Anpassung handeln, denn laut dem Bundesrat handelt es sich bei der Richtlinie um ein Spezialgesetz zur DSGVO und damit nicht um eine Schengen-Weiterentwicklung.[60]

In der Schweiz ist der Schutz der elektronischen Kommunikation schon jetzt vorgesehen, und zwar sowohl in den spezifischen Vorschriften des schweizerischen Fernmeldegesetzes (FMG)[61] als auch in den allgemeineren Regelungen des Datenschutzgesetzes (DSG) oder des Zivilgesetzbuches. Es ist zu erwarten, dass die zuständigen Behörden, namentlich das Bundesamt für Justiz (BJ) sowie das Bundesamt für Kommunikation (BAKOM) diesbezüglich die Entwicklung in der Union verfolgen, die Tragweite der neuen Schutzmassnahmen im Bereich der elektronischen Kommunikation analysieren und nach dem Erlass der Verordnung voraussichtlich im Jahr 2018 bestimmen, ob die Schweizer Gesetzgebung dannzumal in spezifischen Gebieten anzupassen ist. Jedenfalls wird seitens der beteiligten Behörden im Moment kein Handlungsbedarf gesehen.[62]

Erwähnt sei ausserdem, dass die Schweiz im *Datenschutzausschuss des Europarates* Einsitz hat, „der sich mit der Modernisierung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten beschäftigt. Sie nimmt zudem an den Sitzungen der DAPIX-Expertengruppe des Ministerrates teil, die mit der Untersuchung der neuen EU-Datenschutzvorschriften beauftragt ist."[63]

4.2.
Wie erwähnt (siehe 4.1.), geht dieser Bericht davon aus, dass die DSGVO in der Schweiz als EU-Drittstaat nicht direkt anwendbar ist, nicht im Bereich der Daten-

[58] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM(2017) 10 final.
[59] Die Schweiz und der digitale Binnenmarkt der EU (Fn. 25), S. 17.
[60] Botschaft (Fn. 48), S. 25.
[61] Fernmeldegesetz (FMG) vom 30. April 1997, SR 784.10, https://www.admin.ch/opc/de/classified-compilation/19970160/index.html (zuletzt besucht: 30.9.2017).
[62] Die Schweiz und der digitale Binnenmarkt der EU (Fn. 25), S. 17.
[63] Ebenda.

bearbeitung durch die Behörden und in jedem Fall nicht im Bereich der Datenbearbeitung durch Private. Zahlreiche schweizerische Unternehmen sind aber von den Bestimmungen der DSGVO dennoch unmittelbar betroffen und zwar in zweifacher Hinsicht:[64]

- Zum einen gilt das *Niederlassungsprinzip*. Die DSGVO wendet sich auf alle Datenbearbeitung im Rahmen der Tätigkeiten der EU-Niederlassungen von schweizerischen Mutterunternehmen an (Art. 3 Abs. 1 DSGVO). Angesichts der Komplexität der Unternehmensprozesse und der verwendeten IT-Systeme lassen sich Datenbearbeitungen der EU-Niederlassungen einer in einem EU-Drittstaat domizilierten Unternehmung rasch einmal nicht mehr von der Datenbearbeitung ausserhalb der EU trennen. Insofern dürften sich die Massnahmen zur DSGVO-Compliance darüber hinaus auch auf die Datenbearbeitung im Rahmen der Geschäftstätigkeit ausserhalb der EU auswirken.
- Zum zweiten ist das *Marktortprinzip* zu beachten. Die DSGVO ist von der grossen Zahl schweizerischer Unternehmen einzuhalten, die betroffenen Personen in der Union Waren oder Dienstleistungen anbieten oder dort das Verhalten von betroffener Personen beobachten (Art. 3 Abs. 2 DSGVO).

Umgekehrt sind Unternehmensgruppen, die ihre Hauptniederlassung gemäss Art. 4 Ziff. 13 DSGVO in der Schweiz und nicht in einem EU-Land domiziliert haben, unter Umständen *vom Vorteil des sogenannten One-stop-shop-Prinzips ausgeschlossen* (Art. 56 DSGVO). Mit anderen Worten gibt es für diese keine federführende Aufsichtsbehörde, die „einzige Ansprechpartner[in] der Verantwortlichen oder der Auftragsverarbeiter für Fragen der von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführten grenzüberschreitenden Verarbeitung" ist (Art. 56 Abs. 6 DSGVO). Sie müssen vielmehr über ihre örtliche Niederlassung oder Vertretung mit den lokalen Aufsichtsbehörden in jedem Mitgliedstaat in Verbindung treten, in dem sie tätig sind.[65] Ganz sicher ist dies der Fall, wenn die DSGVO Anwendung findet und das Unternehmung aber keine Niederlassung in der EU hat.[66] Die daraus resultierende

[64] Vgl. etwa Lukas Bühlmann/Michael Reinle, ‚Extraterritoriale Wirkung der DSGVO', *digma* 2017, 8-12.

[65] Article 29 Working Party, Guidelines for identifying a controller or processor's lead supervisory authority, adopted on 13.12.2016, http://ec.europa.eu/newsroom/document.cfm?doc_id=44102 (zuletzt besucht: 30.9.2017), S. 7 f.

[66] Article 29 Working Party, Guidelines for identifying a controller or processor's lead supervisory authority (Fn: 65), S. 9: "The GDPR's cooperation and consistency mechanism only applies to controllers with an establishment, or establishments, within the European Union. If the company does not have an establishment in the EU, the mere presence of a representative in a Member State does not trigger the

Verzettelung dient jedenfalls nicht der von der neuen EU-Regelung angestrebten einheitlichen Anwendung der Bestimmungen der Verordnung (Erw. 123 in der Präambel der DSGVO). Zudem es liegt auf der Hand, dass gerade dann, wenn bei grösseren Unternehmensgruppen die Datenbearbeitung eine grosse Zahl oder gar alle EU-Mitgliedstaaten betrifft, ein sich mehrfach duplizierender und dadurch unproduktiver Verwaltungsaufwand anfällt.[67] Schweizerische Unternehmen fühlen sich deshalb benachteiligt.[68] Das schweizerische Parlament hat dies aufgenommen und im Sommer 2017 einen Vorstoss gutgeheissen, der auf eine staatsvertragliche Regelung mit der EU zur Vermeidung der administrativen Doppelspurigkeiten abzielt.[69]

In der Praxis besteht weiter eine Herausforderung darin, dass die schweizerischen *Unternehmen von den neuen unionsrechtlichen Anforderungen rechtzeitig Kenntnis erhalten und dann auch entsprechende Schritte unternehmen*. Auf die Relevanz der neuen Anforderungen nach der DSGVO für Schweizer Unternehmen wird in zahlreichen, v.a. an die Unternehmen gerichteten Publikationen hingewiesen.[70] Eine wichtige Rolle nehmen dabei die Wirtschaftsprüfer ein, die ihre Kunden auf die durch die DSGVO entstehenden Risiken und Prüfpflichten hinweisen.[71] Auch über wissenschaftliche Kanäle werden die Unternehmen davor gewarnt, mit Blick auf die neuen europarechtlichen Anforderungen einfach nichts zu unternehmen. Stattdessen werden ihnen praktische Anleitungen inkl. 12 Punkte-Selbsttest

one stop shop system. This means that controllers without any establishment in the EU must deal with local supervisory authorities in every Member State they are active in, through their local representative."

[67] In praktischer Hinsicht ist zudem anzumerken, dass die jeweilige Ländervertretung des Datenbearbeiters angesichts der zentralisierten Struktur der Geschäftsprozesse in international tätigen Unternehmen in der Regel über sehr viele Aspekte der betreffenden Bearbeitung gar keine Kenntnis hat, insbes. wenn sie vor allem Vertriebsfunktionen wahrnimmt. Genau dies aber wäre für eine effizienten Rechtsdurchsetzung Voraussetzung (Erw. 129 in der Präambel der DSGVO).

[68] David Rosenthal, ‚Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet', in: *Jusletter* 20. Februar 2017, Rz. 130 ff.; David Rosenthal, EU Datenschutz-Grundverordnung, Die Auswirkungen auf Schweizer Unternehmen, 31.8.2016, S. 7, http://www.homburger.ch/fileadmin/Data_Protection/2016-08-31_Homburger_DSGVO_kurz.PDF (zuletzt besucht: 30.9.2017).

[69] Motion 16.3752, Doris Fiala, Gegen Doppelspurigkeiten im Datenschutz, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163752 (zuletzt besucht: 30.9.2017).

[70] Statt vieler etwa Ursula Widmer, ‚Datenschutz: Was uns das EU-Recht angeht. Viele Schweizer Unternehmen wissen vermutlich noch gar nicht, dass sie von der kommenden EU-Datenschutzverordnung betroffen sind', ComputerWorld 6/2016, 62-65, sowie Giorgio V. Müller, ‚EU-Datenschutzverordnung tangiert auch die Schweiz. Kaum ein Schweizer Unternehmen, das nicht vom neuen Datenschutzgesetz betroffen ist, das nächsten Mai in der EU zur Anwendung kommt. Die Regulierung zwingt Firmen, den Datenschutz ernst zu nehmen.', Neue Zürcher Zeitung vom 14.7.2017.

[71] Statt vieler KPMG Schweiz, Datenschutz-Compliance, 5 Juli 2017: „Matthias Bossardt und Jutta Sonja Oberlin erläutern in ihrem Fachartikel für das Magazin „Compliance Berater" die Compliance-Auswirkungen der neuen EU-Datenschutzgrundverordnung (GDPR)", https://home.kpmg.com/ch/de/home/themen/2017/07/data-protection-compliance.html (zuletzt besucht: 30.9.2017).

an die Hand gegeben (Rosenthal)[72] oder empfohlen, anhand einer *to do*-Liste vorab einen Kommunikations- und Krisenplan zu erstellen (Beranek Zanon).[73] Dabei zeigte sich, dass zumindest z.B. mit Bezug auf die Meldepflicht zwischen der EU-DSGVO und dem schweizerischen Vorentwurf Unterschiede bestanden, welche es – würden sie fortbestehen – den Unternehmen nicht unbedingt einfacher machen.[74]

Schliesslich befassen sich die Wirtschaftsverbände in ihren internen Arbeitsgruppen mit den Auswirkungen der Datenschutzentwicklung in der Union,[75] versorgen ihre Mitglieder mit relevanten Informationen und entwickeln entsprechende Best Practices für die schweizerischen Unternehmen. Dabei werden besonders kleinere Unternehmen zusätzlich auch vom Staatssekretariat für Wirtschaft SECO unterstützt, die durch den Datenschutz neu hervortretenden Anforderungen zu verstehen und in den Arbeitsprozessen wie auch in der Produktgestaltung umzusetzen.[76]

4.3.

Der juristische Diskurs zur Digitalisierung ist in der Schweiz tendenziell erst am Anlaufen (siehe dazu auch in der Einleitung zum vorliegenden Bericht). Besonders hervorzuheben sind aber die Entwicklungen betreffend die allgemeine Datenpolitik des Bundes als Basis für die künftige Regulierung des Umgangs mit Daten, die Frage nach dem Eigentum an Daten sowie die Debatte um die Notwendigkeit und Ausgestaltung von E-Identitäten.

[72] David Rosenthal, ‚Datenschutz-Compliance im Unternehmen: Eine etwas andere Anleitung …', in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Datenschutz-Managementsysteme im Aufwind?, ZIK – Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich Band/Nr. 62, Zürich: Schulthess 2016, 7.29.

[73] Nicole Beranek Zanon, ‚Melde- und Benachrichtigungspflichten nach EU DSGVO + rev. DSG. ToDo Liste für den Notfall', *Jusletter* 2.10.2017.

[74] Zu den Unterschieden etwa Jan Kleiner, ‚Meldepflicht bei Datenschutzverletzungen', *digma* 2017, 170-175; David Vasella/Jacqueline Sievers, ‚Der «Swiss Finish» im Vorentwurf des DSG, *Digma* 2017, 44-49, sowie Jutta Sonja Oberlin/Matthias Bossardt, ‚Datenschutz-Compliance: Die Anforderungen der EU-DSGVO und des VE-DSG der Schweiz', *CB* 2017, 245-249, S. 245.

[75] Siehe statt vieler etwa Wirtschaftsdachverband economiesuisse, Datenschutz ohne Blockade!, https://www.economiesuisse.ch/de/artikel/datenschutz-ohne-blockade (zuletzt besucht: 30.9.2017) sowie SwissHoldings, Datenschutzreform – Gefahr oder willkommene Reform?, http://www.swissholdings.ch/fileadmin/kundendaten/Dokumente/Themen_sowie_Anlagen_News/Compliance/JB_2017_Datenschutzreform.pdf (zuletzt besucht: 30.9.2017).

[76] Siehe Liste der 2017 im KMU-Forum behandelten Themen, https://www.seco.admin.ch/seco/de/home/Standortfoerderung/KMU-Politik/KMU-Forum_KMU-Test/behandelte-themen.html (zuletzt besucht: 30.9.2017).

Allgemeine Datenpolitik des Bundes

Am 22.2.2017 definierte der Bundesrat (Schweizer Bundesregierung) die *übergeordneten Ziele einer nationalen Datenpolitik* und beauftragte zugleich die Bundesverwaltung, bis Ende 2017 die Eckdaten zu einer Datenpolitik zu erstellen.[77] Bis dann sollen dazu unter anderem die Rechtslage für eine Weiterverwendung von Personendaten, Sachdaten und anonymisierten Daten analysiert, die Datenbestände des Bundes inventarisiert und für die Publikation als open data geeignete Daten identifiziert werden. Zugleich stellte der Bundesrat fest, „dass Daten der Rohstoff einer digitalen Wirtschaft und Gesellschaft sind. Geeignete Datenbestände sollen deshalb für eine Wiederverwendung zur Verfügung stehen."[78] Damit gab er wohl ein Signal zugunsten einer modernen Auffassung zum Datenschutz, gemäss der Personendaten nicht absolut geschützt sind, sondern bei zureichenden Vorkehrungen zum Schutz der Persönlichkeit und der Transparenz auch weiteren Interessen dienen können.

Eigentum und Zugang zu Daten

Die rechtliche Diskussion zum Thema „Eigentum und Zugang zu Daten" verdichtet sich in der Schweiz zu zwei Fragekreisen:

Zum einen wird erörtert, ob ein Bedürfnis nach *sachenrechtlichem Eigentum* an Daten bestehe. Die Befürworter stellen, insbesondere auch im Zusammenhang mit der Einordnung von Kryptowährungen, die dadurch zu erlangende Rechtssicherheit in den Vordergrund.[79] Dem steht jedoch die wohl überwiegende Ansicht entgegen, dass es für eine dogmatische Festlegung noch zu früh sei, namentlich, weil die gesellschaftlichen und technischen Auswirkungen der Datenwirtschaft noch gar nicht zuverlässig genug abgeschätzt werden könnten, dass sich eine tragfähige Rechtsüberzeugung herausgebildet hätte.[80] Parallel zur Eigentumsfrage

[77] Medienmitteilung des Bundesrats vom 22.3.2017: Auf dem Weg zu einer Datenpolitik des Bundes, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-66068.html (zuletzt besucht: 30.9.2017).

[78] Ebenda.

[79] Statt vieler Martin Eckert, ‚Digitale Daten als Wirtschaftsgut: Daten als Sache', *Schweizerische Juristen-Zeitung* 2016, 245-249, S. 246 und 249, sowie Martin Eckert, ‚Digitale Daten als Wirtschaftsgut: Besitz und Eigentum an Daten', *Schweizerische Juristen-Zeitung* 2016, 265-274, S. 273, mit weiteren Hinweisen.

[80] Siehe statt vieler: Gianni Fröhlich-Bleuler, ‚Eigentum an Daten?', in: *Jusletter* 6.3.2017, http://jurpm.ch/fileadmin/user_upload/files/pdf/zur_person/Jusletter_eigentum_an_daten.pdf (zuletzt besucht: 30.9.2017), S. 10; weiter Center for Information Technology, Society, and Law (ITSL), University of Zurich, Workshop Summary, International Exploratory Workshop on Data Ownership, 6. – 8.7.2017, http://www.itsl.uzh.ch/dam/jcr:1a3604c6-04b0-47ef-92a8-a329edf191ee/Workshop%20Summary.pdf (zuletzt besucht: 30.9.2017), S. 2, sowie Einladung zur Fachtagung Schweizer Forum für Kommunikationsrecht, ‚Dateneigentum und Datenzugang: Herausforderungen in der Praxis', 29.11.2017, http://www.sf-fs.ch/files/sf-fs__itsl__flyer_dateneigentum_und_datenzugang_2.pdf (zuletzt besucht: 30.9.2017), S. 1. In dieser letztgenannten Quelle kommt eine eher kritische Einschätzung zum Ausdruck: „Das Center for

wird namentlich auch über die rechtlichen Problemstellungen um den Einsatz von *distributed ledger*-Technologien (und spezifischer *Blockchain*-Technologien) im Industrie-, Finanz- und generell im Dienstleistungsbereich engagiert diskutiert.[81]

Zum anderen wird nach den rechtlichen Rahmenbedingungen gesucht, unter denen in Ausübung hoheitlicher Aufgaben und unter Einsatz öffentlicher Gelder angefallene oder spezifisch erhobene Daten in der *für das Gemeinwohl zuträglichsten Art und Weise verfügbar gemacht* werden können. Schon länger fordern die Nutzerseite bzw. die Wirtschaftsverbände unter dem Programmbegriff „Open Government Data" die aktive Veröffentlichung von Behördendaten und ähnlicher staatlicher Datensammlungen in maschinenlesbarer Form zur möglichst freien Wiederverwendung.[82] Am 16.4.2014 genehmigte der Bundesrat einen ersten Bericht über die Open-Government-Data-Strategie Schweiz 2014–2018, der unter Angleichung an die internationale Entwicklung Freigabe, koordinierte Publikation und Bereitstellung geeigneter Behördendaten sowie die Etablierung einer eigentlichen Open-Data-Kultur postulierte.[83] In diesem Sinn erklärte er schliesslich im Frühling 2017 die Nutzung der digitalen Datenbestände als Rohstoff für Gesellschaft und Wirtschaft zu einem Eckpfeiler seiner künftigen Datenpolitik.[84]

Die juristischen Fragestellungen um Eigentum und Besitz an Daten und die Regulierung des Zugangs zu diesen wird regelmässig in internen Arbeitsgruppen der Industrie und der Wirtschaftsverbände sowie an Fachtagungen[85] erörtert.

Information Technology, Society and Law (ITSL) der Universität Zürich hat diese Frage im Rahmen eines Forschungsprojekts untersucht und ist zum vorläufigen Schluss gekommen, dass die Einführung eines allgemeinen „Dateneigentums" nach heutigem Kenntnisstand kaum sinnvoll wäre. Damit ist die Sache freilich nicht erledigt. Denn zum einen wirft die faktische Herrschaft von Unternehmen über riesige Datenbestände die Frage auf, ob in gewissen Konstellationen spezifische Zugangsrechte zu Daten erforderlich sind. Zum anderen bestehen verschiedene praktische Probleme, die allenfalls mit einem allgemeinen „Dateneigentum" gelöst werden könnten und die nun andere Lösungen erfordern." – Dieser letztere Einschätzung begegnet der Autor des vorliegenden Berichts auch weit überwiegend in Fachgesprächen in Unternehmenskreisen, in der Wissenschaft und mit Behörden.

[81] Siehe statt vieler: Mirjam Eggen, ‚Chain of Contracts, Eine privatrechtliche Auseinandersetzung mit Distributed Ledgers', *Aktuelle Juristische Praxis* 2017, 3-15, mit weiteren Hinweisen.

[82] Vgl. Open Government Data für die Schweiz – Ein Manifest, Version 1.0, 3.5.2011, https://opendata.ch/organisation/manifest (zuletzt besucht: 30.9.2017). Siehe später auch economieuisse, Zukunft digitale Schweiz, Wandel gemeinsam gestalten (Fn. 27), S. 81 und 89.

[83] ISB – Informatiksteuerungsorgan des Bundes, Open-Government-Data-Strategie Schweiz 2014–2018, vom Bundesrat am 16.4.2014 genehmigt, https://www.admin.ch/opc/de/federal-gazette/2014/3493.pdf (zuletzt besucht: 30.9.2017).

[84] Medienmitteilung des Bundesrats vom 22.3.2017 (Fn. 77).

[85] Siehe statt vieler: SwissIGF, Swiss Internet Governance Forum, 30.5.2017, http://swiss-igf.ch/programm zzzz oder die Fachtagung Schweizer Forum für Kommunikationsrecht, ‚Dateneigentum und Datenzugang: Herausforderungen in der Praxis' (Fn. 80).

Insbesondere letztere dienen als wichtige Austauschplattform zwischen Behörden, Technologieanbietern, Unternehmen, Wirtschaftsberatung und Advokatur.

Elektronische Identität

Geschäftsprozesse werden zunehmend auf elektronischem Wege abgewickelt. Um wichtige Transaktionen im Internet abwickeln zu können, müssen sich die Partner auf die Identität ihres Ansprechpartners verlassen können. Eine erste, im Frühling 2015 vom Bundesamt für Polizei (fedpol) anberaumte informelle Konsultation hatte einen breiten Konsens aufgezeigt, dass umgehend ein rechtlicher und organisatorischer Rahmen für die staatliche Anerkennung von *elektronischen Identifikationsmitteln* und deren Anbieter bereitzustellen sei.[86] Gestützt darauf setzte der Bundesrat im Januar 2016 erste Eckwerte für die Regulierung über elektronische Identitäten. Namentlich beschloss er, „für staatlich anerkannte elektronische Identitäten (eID) auf vom Markt entwickelte Systeme" zu setzen:

> „Demnach ist die Herausgabe einer eigenen staatlichen eID durch den Bund nicht mehr vorgesehen. Diese wäre der schnellen und dynamischen Entwicklung der Technologie und dem Verhalten der Nutzerinnen und Nutzern nicht gewachsen und stünde in Konkurrenz zu innovativen Lösungen des Marktes. Stattdessen will sich der Bundesrat darauf konzentrieren, die rechtlichen und technischen Rahmenbedingungen zu definieren. Diese ermöglichen es den Identitätsdienstleistern, ihre eID-Systeme staatlich anerkennen zu lassen. So ist sichergestellt, dass wirtschaftlich erfolgreiche eID-Systeme auf den Markt kommen und sich den technologischen Entwicklungen rasch anpassen können."[87]

Nach weiteren Vorarbeiten eröffnete der Bundesrat schliesslich am 22.2.2017 eine formelle Vernehmlassung zu einem Vorentwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz).[88] Der Vorentwurf ging in Umsetzung der Eckwerte von einer Aufgabenteilung zwischen Staat und Markt aus:

[86] Bundesamt für Polizei, Zusammenfassung der Ergebnisse der informellen Konsultation vom 13.5.2015 – 5.6.2015 betreffend „Konzept für schweizerische staatlich anerkannte eID-Systeme", https://www.schweizerpass.admin.ch/dam/data/pass/aktuell/konsultation/d-informelle-konsultation-eID.zip (zuletzt besucht: 30.9.2017), S.1.

[87] Medienmitteilung des Bundesrats: Bundesrat beschliesst weitere Schritte für staatlich anerkannte elektronische Identitäten, 13.01.2016, https://www.schweizerpass.admin.ch/pass/de/home/aktuell/news/2016/ref_2016-01-13.html (zuletzt besucht: 30.9.2017).

[88] Medienmitteilung des Bundesrats: Elektronische Identität: Bundesrat will den nötigen Rahmen schaffen, 22.2.2017, https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2017/2017-02-22.html (zuletzt besucht: 30.9.2017).

> „Konkret sollen geeignete private oder öffentliche Identifizierungsdienstleister von einer Anerkennungsstelle auf Bundes-Ebene eine Zulassung zur Herausgabe von staatlich anerkannten elektronischen Identifizierungsmitteln erlangen können."[89]

Das Konzept soll dabei explizit auf Vereinbarkeit mit ähnlichen e-ID-Systemen in anderen Ländern und Regionen ausgelegt sein.[90] Soweit sich dies überblicken lässt, dürfte der Vorschlag, eine Regelung zu treffen, bei den Konsultationsteilnehmenden unbestritten sein, solange diese geeignet ist, Akzeptanz und Vertrauen zu schaffen. Weniger klar scheint zu sein, ob die E-ID Lösung staatlich oder privat erfolgen soll.[91] Mit einem definitiven Bundesratsentwurf bzw. mit parlamentarischer Behandlung dürfte 2018 zu rechnen sein.

Weitere Aspekte

Wenig diskutiert wird ein eventuelles Recht auf *Datenportabilität*. Dieses wird in Art. 20 DSGVO gesetzt, kommt aber umgekehrt im Europaratsübereinkommen No. 108 auch in seiner revidierten Form gemäss dem Modernisierungsentwurf von 2016 nicht vor. Zumindest im Kontext der laufenden Totalrevision des Schweizer Datenschutzrechts ist mit einer Einführung kaum zu rechnen, obwohl dies der EDÖB gemäss seiner Vernehmlassungsantwort begrüssen würde.[92]

[89] Ebenda.

[90] Der Begleitbericht zum Vorentwurf (Bundesamt für Justiz, Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz), Erläuternder Bericht zum Vorentwurf, https://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/e-id/vn-ber-d.pdf (zuletzt besucht: 30.9.2017), S.13 f.) erläutert: „In Anbetracht der globalen Natur von Online-Diensten im Internet, ist es wichtig, ein vom Staat anerkanntes elektronisches Identifizierungsmittel in konzeptioneller, technischer und rechtlicher Hinsicht so zu gestalten, dass es später international eingesetzt werden kann, insbesondere im europäischen Raum. In der eIDAS-Verordnung und den entsprechenden technischen Standards werden Rahmenbedingungen spezifiziert, die garantieren, dass die Interoperabilität zwischen den einzelnen länderspezifischen Systemen gewahrt wird. Das Konzept für schweizerisch anerkannte E-ID-Systeme richtet sich an diesen internationalen Vorgaben aus, so dass die schweizerischen E-ID auch im internationalen Kontext eingesetzt werden könnten. Unter anderem wird mit dem vorliegenden Gesetz ein Rechts- und Standardisierungsrahmen für die Anerkennung von E-lD-Systemen und die Anerkennung der IdP geschaffen. Dieser ist so ausgestaltet, dass eine spätere gegenseitige Anerkennung der E-lD-Systeme zwischen der Schweiz und der EU, oder einzelner Mitgliedstaaten, möglich bleibt. Dazu wären bilaterale Verträge nötig."

[91] So ist der Stellungnahme des Wirtschaftsdachverbands economiesuisse, 29.5.2017, https://www.economiesuisse.ch/sites/default/files/publications/20170529_Website_Stellungnahme_E-ID-Gesetz.pdf (zuletzt besucht: 30.9.2017) zu entnehmen: „Akzeptanz hängt stark vom Vertrauen ab. Dieses jedoch hängt nicht primär von der Frage ab, ob ein privater oder staatlicher Herausgeber die E-ID anbietet. Die Meinungen, ob die E-ID Lösung staatlich oder privat erfolgen soll, sind im Kreise unserer Mitglieder denn auch uneinheitlich. Der Blick ins Ausland zeigt, dass sowohl staatliche als auch private Lösungen das Potenzial haben, sich durchzusetzen oder zu scheitern. Vertrauen kann gerade auch durch private und breit akzeptierte Anbieter geschaffen werden. "

[92] EDÖB, Zur Botschaft über die Totalrevision des Datenschutzgesetzes des Bundes vom 15.9.2017, https://www.edoeb.admin.ch/aktuell/01468/index.html?lang=de (zuletzt besucht: 30.9.2017).

Der Bundesrat will jedoch die Erfahrungen innerhalb der Europäischen Union abwarten und dann insbesondere im Zusammenhang mit der Umsetzung der Gesamtstrategie „Digitale Schweiz“[93] die Einführung eines Rechts auf Datenportabilität neu prüfen.[94]

Im Anlaufen sind dagegen regulatorische Diskussionen zur *Stabilisierung des Arbeitsmarkts zufolge der Robotorisierung*[95] sowie zu den *wettbewerbsrechtlichen Aspekten von Buchungsplattformen*. Zu letzteren warnt die schweizerische Wettbewerbsbehörde (WEKO) vor voreiliger Regulierung.[96] Allerdings hat das das Parlament jüngst einen Vorstoss zur Regulierung von sogenannten Preisparitätsklauseln im Vertragsverhältnis zwischen Online-Buchungsplattformen und Hotels im Prinzip angenommen.[97]

4.4.

Die im vorliegenden Zusammenhang relevante EuGH-Entscheidung *Google gegen Spanien*[98] bezieht sich auf die Richtlinie 95/46, welche – wie oben erwähnt (siehe 4.1.) – im Rahmen der Schengen- und Dublin-Assoziation der Schweiz auch für dieses Land relevant ist. Das Thema ist aber von grösserer Tragweite, wie die folgenden Ausführungen zeigen.

In der Schweiz geben der verfassungsmässige *Schutz der persönlichen Freiheit* und die dazu bestehenden einklagbaren Ansprüche nach Art. 27 ff. Zivilge-

[93] Botschaft (Fn. 48), S. 17 und 71.

[94] Botschaft (Fn. 48), S. 46.

[95] Siehe statt vieler: Tibère Adler/Marco Salvi, Wenn die Roboter kommen. Den Arbeitsmarkt für die Digitalisierung vorbereiten, avenir suisse, 4.10.2017, https://www.avenir-suisse.ch/publication/wenn-die-roboter-kommen (zuletzt besucht: 30.9.2017), mit weiteren Hinweisen.

[96] Zwar hatte die Wettbewerbsbehörde nach einer Untersuchung 2015 den Buchungsplattformbetreibern verboten, die Hotels in ihrer Angebotspolitik umfassend einzuschränken; siehe Medieninformation WEKO, WEKO verbietet Hotelbuchungsplattformen wettbewerbsbeschränkende Klauseln, 6.11.2015, https://www.weko.admin.ch/weko/de/home/aktuell/medieninformationen/nsb-news.msg-id-59358.html (zuletzt besucht: 30.9.2017). In einem neuen Zeitungsinterview meint aber Rafael Corazza, Direktor der WEKO, unter Bezug auch auf Dienste wie Uber, in: Neue Zürcher Zeitung, Ohne die Wettbewerbskommission hätten die Hoteliers keinen Schutz, 30.9.2017, https://www.nzz.ch/schweiz/ohne-uns-haetten-hotels-keinen-schutz-ld.1320170 (zuletzt besucht: 30.9.2017): „*Bei Booking hat sich das Parlament entschieden, den Fall selbst zu lösen – mit einem Gesetz auf nationaler Ebene. Befürchten Sie dass die Politik hier zunehmend eingreifen wird?* Nein, bis jetzt gibt es keine derartigen Anzeichen. Aber wir sollten auf der Hut sein. Interessengetriebene Spezialgesetze können Anreize zur Innovation gefährden. Vergessen wir darum nicht, welche Fortschritte und Effizienzgewinne wir durch die Digitalisierung der Wirtschaft erhalten.“

[97] Motion 16.3902, Pirmin Bischof, Verbot von Knebelverträgen der Online-Buchungsplattformen gegen die Hotellerie, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163902 (zuletzt besucht: 30.9.2017).

[98] EuGH, Rs. C-131/12 *Google Spain SL and Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González*, ECLI:EU:C:2014:31.

setzbuch (ZGB)[99] dem Einzelnen schon seit Langem Rechtsinstrumente in die Hand, um sich gegen eine als unverhältnismässig empfundene Verbreitung von Information über die eigene Person zur Wehr setzen zu können. Der schweizerische Ansatz gegenüber dem Recht auf Vergessen ist vor dem Hintergrund dieser Tradition zu verstehen.

Vor allem im *klassischen Pressebereich* zeigte sich parallel zum Justizweg schon vor dem Aufkommen der sozialen Medien das Bedürfnis, in einem alternativen Verfahren Fragen um das Erheben, Verbreiten und Löschen persönlicher Daten zu regeln. Im Rahmen dieses alternativen Verfahrens hat der Schweizerische Presserat[100] im Licht des Schweizer Journalistenkodex (Erklärung der Pflichten und Rechte der Journalisten)[101] eine eigene Spruchpraxis entwickelt. Diese bezieht sich u.a. auf die Pflicht 7 über den Respekt der Geheimsphäre. In seinen Entscheiden Nr. 22/2008[102] und 5/2009[103] äusserte sich der Presserat schon früh auch zum Recht auf Vergessen. Allerdings wurde in beiden Fällen dem Interesse der Öffentlichkeit gegenüber dem individuellen Interesse auf Wahrung der Privatsphäre der Vorzug gegeben. Der Presserat nimmt heute eine differenzierte Haltung ein. Gemäss „Richtlinie 7.5 – «Recht auf Vergessen»" in den Richtlinien zur «Erklärung der Pflichten und Rechte der Journalistinnen und Journalisten» geniessen

> „Verurteilte ein «Recht auf Vergessen». Dies gilt erst recht bei Einstellung eines Verfahrens und bei Freispruch. Das «Recht auf Vergessen» gilt aber nicht absolut. In verhältnismässiger Art und Weise dürfen Journalistinnen und Journalisten über frühere Verfahren berichten, sofern ein überwiegendes öffentliches Interesse dies rechtfertigt. Beispielsweise, wenn ein Zusammenhang zwischen früherem Verhalten und aktueller Tätigkeit besteht.
>
> «Das ‹Recht auf Vergessen» gilt auch für Online-Medien und digitale Archive. Redaktionen sollten auf begründetes Gesuch hin prüfen, ob sich eine nachträgli-

[99] Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907, SR 210; https://www.admin.ch/opc/de/classified-compilation/19070042/index.html#a27 (zuletzt besucht: 30.9.2017).

[100] Der Schweizerische Presserat ist vom Verband Schweizer Presse eingesetzt worden. Er wirkt auf privater Basis und ohne Durchsetzungskompetenz als medienethisches Selbstregulierungsorgan der Schweizer Presse; siehe http://www.presserat.ch (zuletzt besucht: 30.9.2017).

[101] Erklärung der Pflichten und Rechte der Journalistinnen und Journalisten, Fassung vom 5.6.2008. http://www.presserat.ch/code_d.htm (zuletzt besucht: 30.9.2017). Der Schweizer Journalistenkodex ist vom Schweizerischen Presserat erlassen worden.

[102] Nr. 22/2008: Suicide d'un prêtre / Traitement des affaires de prêtres pédophiles / Droit à l'oubli Prise de position du Conseil suisse de la presse du 21 mai 2008, http://www.presserat.ch/24070.htm (zuletzt besucht: 30.9.2017).

[103] Nr. 5/2009: Recht auf Vergessen / Anhörung bei schweren Vorwürfen (Steiner c. «20 Minuten») Stellungnahme des Schweizer Presserates vom 15. Januar 2009, http://www.presserat.ch/24800.htm (zuletzt besucht: 30.9.2017).

che Anonymisierung oder Aktualisierung eines elektronisch archivierten Medienberichts aufdrängt. Bei Berichtigungen sollten die Redaktionen einen zusätzlichen Vermerk anbringen, anstatt bloss die vorangehende Version zu überschreiben. Löschungsbegehren sind abzulehnen. Zudem sollten Journalisten ihre Quellen bei Internet- und Archivrecherchen besonders kritisch überprüfen."[104]

In der *schweizerischen juristischen Lehre* werden Doktrin und Praxis zum Recht auf Vergessen bisher nur mässig erörtert. Eine eindeutige Haltung ist nicht auszumachen. Während argumentiert wird, dass ein modern verstandener Datenschutz dem Individuum eine aktive Möglichkeit einräumen sollte, für eine vernünftige Information des Publikums irrelevant gewordene Informationen aus dem öffentlichen Informationsraum entfernen zu können, wird gleichzeitig auch vorhergehoben, dass dem Einzelnen zugemutet werden könne, mit dem Verbreiten von Information über die eigene Person eigenverantwortlich umzugehen. Zugleich wird vorgebracht, dass für den schweizerischen Rechtsraum hier eine gewisse Gestaltungsfreiheit bestehen dürfte, weil eine eigenständige Regelung die Äquivalenz zur EU-Regelung nicht verhindern dürfte, insofern also unproblematisch sei.[105] Die wesentlichen Elemente sind in der schweizerischen Rechtsordnung tatsächlich bereits berücksichtigt. Auf den wissenschaftlichen Diskurs wirkt sich derzeit vor allem verzögernd aus, dass eine eventuelle legislatorische Klärung in der Schweiz gerade erst ansteht und die Kasuistik zurückhaltend ausgebildet ist.[106]

Der *Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB)* empfahl bereits 2011 eine eingehendere Befassung mit dem Recht auf Vergessen. Unter anderem die lange Verfügbarkeit von Daten in den Netzwerken sowie technische Fortschritte führten dazu, dass der betroffenen Person adäquate Mittel zur Sicherung ihrer persönlichen Rechte gegenübergestellt werden sollten.[107] Diese Haltung behält er in seiner aktuellen, nun aber deutlicher ausdif-

[104] Schweizerischer Presserat, Ziffer 7.5 der Richtlinien zur «Erklärung der Pflichten und Rechte der Journalistinnen und Journalisten», Fassung vom 1.7.2017, http://presserat.ch/Documents/Richtlinien_2017.pdf (zuletzt besucht: 30.9.2017). Vergleiche auch Schweizer Presserat, Fragen und Antworten, Antwort 45. Gibt es ein «Recht auf Vergessen»? 30.9.2017, http://ratgeber.presserat.ch/index.php?de_45-gibt-es-ein-arecht-auf-vergessena-1 (zuletzt besucht: 30.9.2017).

[105] Statt vieler: Rolf H. Weber/Ulrike I. Heinrich, ‚Braucht die Schweiz ein Recht auf Vergessen im Internet?', in: Astrid Epiney & Stefan Diezig, *Schweizerisches Jahrbuch für Europarecht 2013/2014*. Zürich: Schulthess 2014, 301-318, mit weiteren Hinweisen.

[106] Siehe etwa Schweizerisches Bundesgericht, BGE 5A_195/2016, 4.7.2016, E. 5.2 mit weiteren Hinweisen. Zur neueren Rechtsprechung des Schweizerischen Bundesgerichts Bruno Baeryswil, ‚Entwicklungen im Datenschutzrecht/Le point sur le droit de la protection des données', *Schweizerische Juristen-Zeitung* 2017, 469-471, S. 470.

[107] Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), 18. Tätigkeitsbericht 2010/2011, 14.6.2011, S. 119, https://www.edoeb.admin.ch/dokumentation/00153/00184/index.html-

ferenzierten Empfehlung zum Recht auf Vergessen bei.[108] Dieses sei zwar nicht als absolutes Recht zu verstehen, sondern verlange im Einzelfall die Interessenabwägung „ob die Verletzung der Persönlichkeitsrechte der von der Datenbearbeitung beziehungsweise Veröffentlichung betroffenen Person durch ein höheres Interesse gerechtfertigt ist oder nicht." Im Internetzeitalter würden aber unter anderem „[d]ie weltweite Datenflut, die technologische Entwicklung (z. B. Gesichtserkennungssysteme, Geolokalisierung, Digitalisierung) und die Arbeitsweise der Suchmaschinen [...] den Kontrollverlust über die eigenen Daten" verschärfen. Dem berechtigten Anliegen des Vergessenwerdens sei durch die Kombination von technischen und rechtlichen Lösungen sowie durch Veränderungen im persönlichen Verhalten, d. h. Sensibilisierung und Eigenverantwortung, Rechnung zu tragen. Dabei sollten auch die Nutzer, die ihre Daten im Internet, insbesondere in sozialen Netzen, zur Verfügung stellen, ihrer Eigenverantwortung bewusst wahrnehmen:

> „Die Internetuser müssen sich der Gefahren im Umgang mit dem Internet bewusst sein und die neuen Technologien verantwortungsvoll einsetzen. Besondere Vorsicht ist bei der Veröffentlichung persönlicher Daten (von sich selber oder von Dritten) im Internet geboten. Diejenigen Personen, die solche Technologien konzipieren und entwickeln, müssen ihrerseits die Datenschutzgrundsätze zum Schutz der Persönlichkeit berücksichtigen und einhalten, indem sie beispielsweise auf eine systematische Indexierung der Daten in Suchmaschinen verzichten. Schliesslich sollten Rechtsprechung und Gesetzgebung die Persönlichkeitsrechte besser schützen und die Pflichten derjenigen, die die Daten bearbeiten, verschärfen."[109]

Auf politischer Ebene wurde 2012 ein auf Einführung eines Rechts auf Vergessen abzielender, parlamentarischer Einzelvorstoss[110] vom Bundesrat und der

?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdYR8fmym162epYbg2c_JjKbNoKSn6A-- (zuletzt besucht: 30.9.2017): „Eine der grossen Herausforderungen des Internet und der virtuellen Welt liegt in der Verwaltung und der Kontrolle der Daten. Einmal im Netz, bleiben sie u. U. ewig erhalten, und können Gegenstand einer Vielzahl von Bearbeitungen in unterschiedlichen Kontexten werden. Alle Handlungen des Users können ungeachtet seines Aufenthaltsorts registriert und nachverfolgt werden: die rasante Entwicklung der Smartphones verstärkt dieses Phänomen zusätzlich. Man müsste sich überlegen, wie in der virtuellen Welt der realen vergleichbare Rechte garantiert werden können, indem insbesondere das Recht auf Vergessen in den Netzwerken bekräftigt wird und die Mittel zu dessen Gewährleistung bereitgestellt werden (Verfallsfrist der Daten, Desindexierungspflicht, Regelung der Geolokalisierung, das Recht zu surfen, ohne beobachtet und profiliert zu werden, das Recht, sich der Veröffentlichung oder Indexierung von Daten im Internet zu widersetzen usw.)."

[108] Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Erläuterungen zum Recht auf Vergessen, https://www.edoeb.admin.ch/datenschutz/00683/01173/index.html?lang=de (zuletzt besucht: 30.9.2017).

[109] Ebenda, in fine.

[110] Postulat 12.3152, Jean Christophe Schwaab, Recht auf Vergessen im Internet, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20123152 (zuletzt besucht: 30.9.2017).

zuständigen parlamentarischen Kammer grundsätzlich positiv aufgenommen. Zugleich aber wurde auf die sich in Vorbereitung befindliche Modernisierung des schweizerischen Datenschutzrechts verwiesen und eine vertiefte Prüfung des Anliegens in jenem Kontext in Aussicht gestellt.[111] Auch der Bundesratsbericht „Rechtliche Basis für Social Media" vom 10.5.202017 sieht angesichts der laufenden Revision des Datenschutzrechts betreffend ein Recht auf Vergessen keinen andersgearteten Regulierungsbedarf.[112]

Das bereits erwähnte *Europaratsübereinkommen No. 108* in seiner aktuellen Form von 1981 nimmt keinen Bezug auf ein ausdrückliches Recht auf Vergessen. Auch der Entwurfstext für ein modernisiertes Übereinkommen, welcher in diesem Punkt als finalisiert gelten kann, erwähnt ein explizites Recht auf Vergessen nicht.[113] Wohl wollte ein Zwischenentwurf für den Erläuternden Bericht vor der letzten Sitzung des Adhoc Committee on Data Protection (CAHDATA)[114] im Juni 2016 noch eine kombinierte Wirkung verschiedener, im modernisierten Übereinkommen enthaltener Prinzipien als pragmatische Ausgestaltung eines Rechts auf Vergessen verstanden wissen.[115] Die nach dieser Sitzung wei-

[111] Stellungnahme des Bundesrats vom 9.5.2012, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20123152#tab-panel-acc-3 (zuletzt besucht: 30.9.2017): „Das Bundesamt für Justiz führte kürzlich eine umfangreiche Evaluation des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1) durch. Der Bundesrat hat am 9. Dezember 2011 seinen Bericht zu dieser Evaluation verabschiedet und gelangt darin zur Auffassung, dass geprüft werden soll, inwieweit aufgrund der rasant fortgeschrittenen technologischen und gesellschaftlichen Entwicklungen gesetzgeberischer Handlungsbedarf besteht und von welcher Art dieser ist. Im Bericht hat der Bundesrat bereits Zielsetzungen skizziert, welche die gesetzgeberischen Revisionsarbeiten anvisieren. Dazu zählt unter anderem eine Verbesserung der Datenkontrolle und -herrschaft. Im Sinne des Postulates soll in diesem Rahmen auch eine Präzisierung des Rechts auf Vergessen geprüft werden (siehe BBl 2012 350)."

[112] Schweizerische Eidgenossenschaft, Rechtliche Basis für Social Media: Erneute Standortbestimmung, Nachfolgebericht des Bundesrates zum Postulatsbericht Amherd 11.3912 „Rechtliche Basis für Social Media", 10.05.2017, https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/digitale-kommunikation/soziale-medien.html (zuletzt besucht: 30.9.2017).

[113] Europarat, CAHDATA, Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data [ETS No. 108], September 2016, https://rm.coe.int/16806a616c (zuletzt besucht: 30.9.2017).

[114] Agenda CAHDATA, 15./16.6.2016, http://www.coe.int/en/web/data-protection/agenda-cahdata-2016 (zuletzt besucht: 30.9.2017).

[115] Europarat, CAHDATA, Draft explanatory report to the Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data [ETS No. 108], 2.6 2016, S. 16, http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a6170 (zuletzt besucht: 30.9.2017): "82. Furthermore, it should be noted that the specification of the purpose, the conditions for the legitimacy of the processing, the requirements as regards the data quality, the right of rectification or erasure, together with the provision on the length of time for data storage (article 5.4. littera e.), coupled with an effective right to object and the right to withdraw consent, offer an effective level of protection for the data subject. This set of rights and requirements pragmatically corresponds to the effect of what is referred to as a 'right to be forgotten'."

ter bearbeitete Entwurfsversion für den Erläuternden Bericht erwähnt diesen vermuteten Zusammenhang allerdings nicht mehr.[116] Vor diesem Hintergrund und angesichts der Tatsache, dass die vorangegangene breite Konsultation („Vernehmlassung") keine eindeutige Präferenz ergeben hatte,[117] hat der Bundesrat im *Entwurf für ein modernisiertes Schweizer Datenschutzgesetz* nun[118] den Spielraum genutzt. Der E-DSG folgt hier dem bereits im aktuellen Datenschutzgesetz[119] und dem Europaratsübereinkommen No. 108 zugrundeliegenden Ansatz der prinzipienbasierten Datenschutzregulierung[120] und sieht ein Recht auf Vergessen *nicht als eigenes formelles Rechtsinstitut des Datenschutzes* vor. Davon ausgehend, dass nach der schweizerischen Rechtsordnung das Datenschutzrecht zum einen das von der Bundesverfassung vorgegebene Grundrecht auf Schutz der Privatsphäre (Art. 13 BV)[121] und zum andern den zivilrechtlichen Persönlichkeitsschutz (Art. 28 ff. ZGB). konkretisiert,[122] erläutert die Botschaft, dass die relevanten Schutzaspekte des Rechts auf Vergessen bereits aufgrund des zivilen Persönlichkeitsrechts gegeben seien:

> „Ein solches Recht auf Vergessenwerden gilt indessen nicht absolut [der Text verweist hier in einer Fussnote auf BGE 111 II 209 E. 3c]. Vielmehr wird in der Rechtsprechung zum Persönlichkeitsschutz grundsätzlich das Interesse der betroffenen Person abgewogen gegen die Meinungs- und Informationsfreiheit, aus denen sich regelmässig ein überwiegendes Interesse am Fortbestehen bzw. an der Verwendung der Information ergibt. Ein solches Interesse kann beispielsweise bestehen bei Archi-

[116] Europarat, CAHDATA, Draft explanatory report to the Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data [ETS No. 108], August 2016, S. 14, https://rm.coe.int/16806b6ec2 (zuletzt besucht: 30.9.2017).

[117] Botschaft (Fn. 48), S.43 f.

[118] Entwurf Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (Fn. 50).

[119] Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992, SR 235.1, https://www.admin.ch/opc/de/classified-compilation/19920153/index.html (zuletzt besucht: 30.9.2017).

[120] Europarat, CAHDATA, Draft explanatory report to the Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data [ETS No. 108], August 2016, S. 6 ff., https://rm.coe.int/16806b6ec2 (zuletzt besucht: 30.9.2017).

[121] Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101, https://www.admin.ch/opc/de/classified-compilation/19995395/index.html#a13 (zuletzt besucht: 30.9.2017).

[122] Zum Ganzen siehe Eva Maria Belser/Hussein Noureddine, in: Eva-Maria Belser/Astrid Epiney/Bernhard Waldmann, *Datenschutzrecht,* Bern: Stämpfli 2011, §7 N17 ff., sowie Sylvain Métille, *Internet et droit: Protection de la personnalité et questions pratiques,* Zürich: Schulthess 2017. – Vgl. auch Hausheer/Aebi-Müller, die zutreffend darauf hinweisen, dass sich die Grenze zwischen Privat- und Gemeinsphäre mit der Zeit verschiebt und daher ein vorher zum Gemeinbereich gehörendes Ereignis von der Bevölkerung regelmässig vergessen wird und damit in den Privatbereich der betroffenen Person übergeht; Heinz Hausheer/Regina E. Aebi-Müller, *Das Personenrecht des Schweizerischen Zivilgesetzbuches*, 4. Auflage, Bern: Stämpfli 2016, N. 12.118.

ven oder Bibliotheken, deren Aufgabe es ist, Dokumente unverändert zu sammeln, zu erschliessen, zu erhalten und zu vermitteln. Besteht ein überwiegendes Interesse, ist die Persönlichkeitsverletzung gerechtfertigt und ein allfälliger Anspruch auf Löschung entfallt. Die notwendige Interessenabwägung im Einzelfall ist aufgrund von Artikel 28 Absatz 2 E-DSG sowie der Verweisung auf die Klagen nach Artikel 28 f. ZGB möglich und erforderlich, sodass keine spezifischen Vorbehalte in den Gesetzestext eingefügt werden müssen."[123]

Auf dieser Basis wäre auch in der Schweiz eine ähnliche Entscheidung denkbar, wie ihn der Gerichtshof der Europäischen Union im Jahr 2014 in der eingangs zu dieser Frage erwähnten Rechtssache *Google gegen Spanien* gefällt hat.[124]

Immerhin und obgleich sich dies implizit bereits aus dem bisherigen Recht ergibt, sieht der E-DSG hingegen *ausdrücklich Bestimmungen betreffend Löschung* vor: Bezüglich der Datenbearbeitung durch private Personen erfolgt dies mittels Verweisung auf die Klagen zum Schutz der Persönlichkeit gemäss den Art. 28, 28a sowie 28g-28l des Zivilgesetzbuchs (Art. 28 Abs. 2 Bst. c E-DSG). Bei der Datenbearbeitung durch Bundesorgane wird ein leicht anderes Konzept gewählt. Dort soll unter bestimmten Bedingungen ein verfahrensmässig eigenständiger Anspruch auf Löschung bestehen (Art. 35 Abs. 2 ff. E-DSG).[125] Die Anforderungen von Art. 8 Bst. e E-Europaratsübereinkommen No. 108[126] sind damit eingehalten. Zugleich ist auch die Annäherung an Art. 17 DSGVO gegeben.

Ein Sonderfall ist schliesslich in Art. 16 Abs. 3 E-DSG betreffend die Löschung von *Daten von verstorbenen Personen angesprochen*. Damit soll die Rechtslage derjenigen von lebenden Personen angenähert werden, wie sie in Artikel 28 E-DSG vorgesehen ist.[127] Der besonderen Situation wird aber mit einer Reihe von spezifischen Vorbehalten Rechnung getragen.

[123] Botschaft (Fn. 48), S. 142 f.
[124] Idem, S. 142.
[125] Idem, S. 149 f.
[126] Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data [ETS No. 108], September 2016 (Fn 52).
[127] Idem, S. 112 f.

THE NETHERLANDS

Lucky Belder • Harrie Temmink*

1. Internal Market and electronic commerce: Internet and e-commerce

1.1. Electronic commerce, liability of Internet intermediaries

Question 1.1.1.

The definition of intermediary services as provided for in Articles 12-14 of the E-Commerce Directive were essentially copied into Article 6:196c of the Dutch Civil Code ("*DCC*"). The latter provides liability exemptions for transmission, caching, and hosting of information provided by others. These liability exemptions protect intermediaries against liability for damages only. As with the E-Commerce Directive, Article 6:196c(5) of the DCC makes clear that intermediaries may still be subject to injunctions, without providing legal grounds upon which such an injunction can be based. In this regard, the question on the definition of intermediary has been primarily focussed on the liability that intermediaries may incur for damages, as opposed to the other forms of action taken against intermediaries (for instance, through injunctions). However, just as in many other EU countries, most of the controversies and court cases have been about injunctions rather than damages.

The *hosting liability exemption* seems to have the most practical relevance in Dutch law. In particular, it has given rise to some case law in which the scope of the exemption played a role. The exemption may apply to forums or message boards, on which users post information. However, if providers moderate or otherwise check the content that is uploaded by users, Dutch courts have held

* Contributions by: Stefan Kulk, Remy Chavannes, Marco Loos, Lisette den Butter, Abe IJland, Lucky Belder, Stijn van Deursen, Hans Vedder, Hielke Hijmans, Emilie van Hasselt.

that these providers are no longer protected by the exemption because they actively engaged with the user-provided content.[1]

The CJEU made clear in both *Google France/Louis Vuitton* and *L'Oreal/Ebay* that the hosting liability exemption can also apply to non-traditional hosting service providers – service providers that do not merely store information for others but also process that information.[2] Nevertheless, the CJEU stressed that, in order to be covered by the exemption, such an intermediary must provide its services 'neutrally by a merely technical and automatic processing of the data provided by its customers.'[3] Specifically with regard to online marketplaces, the CJEU stated in *L'Oreal/Ebay* that 'the mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability.'[4]

The Dutch Court of Appeal of Leeuwarden applied the CJEU's reasoning in *L'Oreal/eBay* in a case about the Dutch online marketplace 'Marktplaats' (a subsidiary of eBay), and came to the conclusion that this service is covered by the hosting liability exemption in the DCC.[5] The fact that Marktplaats enabled its customers to promote their advertisements on the platform did not take away from that conclusion. Nor did Marktplaats' own advertisements for its platform deprive it of its status as a hosting provider.

If a service provider alters information provided by others, the service provider cannot rely on the liability exemption for hosting. Editing submitted texts and scanning and uploading photos can deprive a service provider of safe harbour protection.[6] Some uncertainty still exists with regard to certain types of algorithmic processing of information provided by others. Such processing is technical in nature, but is not necessarily 'neutral'.[7] In the *Skyscanner* case, the Dutch Court of Appeal of Amsterdam held that a flight comparison website could not rely on the liability exemption for hosting with regard to the information it collected

[1] E.g. Rb. Amsterdam (vzr.) 12 March 2009, LJN BH7529; Rb. Noord-Nederland, 3 July 2013, ECLI:NL:RBNNE:2013:3992. Also see on a video-hosting platform: Rb. Amsterdam 24 November, *LJN* BP6880, par. 4.15 (Kim Holland Productions/123Video).

[2] CJEU 23 March 2010, Joined Cases C-236/08 to C-238/08, ECLI:EU:C:2010:159 (*Google France v. Louis Vuitton Malletier*); CJEU 12 July 2011, C-324/09, ECLI:EU:C:2011:474, par. 113 (*L'Oréal and others v. eBay*).

[3] CJEU 23 March 2010, Joined Cases C-236/08 to C-238/08, ECLI:EU:C:2010:159 (*Google France v. Louis Vuitton Malletier*), par. 114 and 120.

[4] CJEU 12 July 2011, C-324/09, ECLI:EU:C:2011:474, par. 113 (*L'Oréal and others v. eBay*), par. 115.

[5] Hof Leeuwarden 22 May 2012, CR, ECLI:NL:GHLEE:2012:BW6296 (*Stokke/Marktplaats*).

[6] E.g.: Rb. Haarlem 11 January 2006, ECLI:NL:RBSHE:2006:AU9504.

[7] E.g. Hof Amsterdam 7 March 2017, ECLI:NL:GHAMS:2017:739 (*Skyscanner*); and Rb. Amsterdam, 18 December 2013, available at: https://perma.cc/Z53F-4WDR. Also see: T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid voor robots en algoritmes', Nederlands Tijdschrift voor Handelsrecht 2017-3, p. 123.

and processed about available flights. As the website organised and ranked the information, it was 'in a way' editing the stored information.[8]

With regard to the *mere conduit exemption*, it is clear that it covers typical internet access providers. As to whether these intermediaries have any enduring responsibilities, such as the obligation to block particular websites, there is less certainty (see below, Q 1.1.4). There is one case that deals with the applicability of the exemption to a service provider that gave its customers access to Usenet – a newsgroup-based network that can also be used to share files.[9] Because such a provider stores information for others on its servers, the provider could not rely on the exemption for mere conduits. Instead, it was only protected by the hosting liability exemption.[10]

Question 1.1.2.

This question presupposes that the CJEU in *L'Oréal v. eBay* laid down a test for liability, when in fact the CJEU only interpreted the conditions for non-liability. Also, the broader EU law framework on intermediary liability does not lay down a test for liability. The rules in the E-Commerce Directive only negatively affect the liability of intermediaries – negative in the sense that these rules hinge on the absence, rather than the presence, of circumstances that give rise to liability.

The CJEU's decision in *eBay* is, to a large extent, a restatement the CJEU's earlier decision in *Google France v. Louis Vuitton* in which the CJEU clarified that the hosting liability exemption can apply to a search engine with regard to the advertisement space it offers.[11] In interpreting the scope of the exemption, the CJEU in *Google France* held that hosting activities should be of 'a mere technical, automatic and passive nature.' [12] To support this finding, the CJEU referred to recital 42 of the E-Commerce Directive. Strictly speaking, recital 42 of the Directive concerns only the mere conduit and caching exemptions. Although it speaks of the 'exemptions from liability established in this directive', this recital nevertheless contains a clear reference to mere conduit and caching activities.[13] Hosting is addressed in the separate recital 46. In this recital, there is no refer-

[8] Hof Amsterdam 7 March 2017, ECLI:NL:GHAMS:2017:739, par. 3.17 (*Skyscanner).*

[9] Hof Amsterdam, 19 August 2014, ECLI:NL:GHAMS:2014:3435 (News-Service Europe).

[10] Hof Amsterdam, 19 August 2014, ECLI:NL:GHAMS:2014:3435, par. 3.4.5 (News-Service Europe).

[11] CJEU 23 March 2010, Joined Cases C-236/08 to C-238/08, ECLI:EU:C:2010:159 (*Google France v. Louis Vuitton Malletier*).

[12] CJEU 23 March 2010, Joined Cases C-236/08 to C-238/08, ECLI:EU:C:2010:159, par. 113 (*Google France v. Louis Vuitton Malletier*).

[13] Recital 42 of the E-Commerce Directive speaks of activities that are 'limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient.'

ence to 'a mere technical, automatic and passive nature'.[14] It thus seems that the CJEU in *Google France,* inadvertently or not, readjusted the scope of the hosting liability exemption.

The CJEU underlined the neutrality criterion in *eBay*, albeit in a slightly modified form. The CJEU dropped 'passive nature', and spoke only of 'merely technical and automatic processing of the data.'[15] This rephrasing of the neutrality criterion appears to bring the lack of human intervention back to the center stage. Not only are traditional, truly passive hosting providers covered by the exemption, but now intermediaries involved in the storage of information and processing thereof by algorithms and other automatic processes are also likely to benefit from the exemption. In times when intermediaries increasingly curate online information through algorithms, the nuance that *eBay* added to the applicability of hosting exemption appears to make sense.

Question 1.1.3.

Notice-and-take down regimes lay the responsibility for finding and signalling unlawful activities on right-holders and others who are harmed by such activities. If, instead, intermediaries were to actively monitor their services, an unreasonable burden would be placed on these intermediaries that could hamper them in developing their innovative services.[16] This question presupposes that notice-and-take down is in itself an appropriate mechanism to deal with unlawful online information and activities. However, we are of the opinion that notice-and-take down mechanisms can only be appropriate if they are provided with sufficient procedural safeguards to protect against the potential chilling effects that such systems may have on freedom of expression.

The liability exemptions in the E-Commerce Directive incentivize the adoption of notice-and-take down mechanisms by intermediaries by making non-liability dependent on the absence of knowledge or awareness of illegal activities. The EU legal framework does not provide any rules on the modalities of notice-and-take down mechanisms. Rather, it leaves this to Member States who may lay

[14] Recital 46 states that '[i]n order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.'

[15] CJEU 12 July 2011, C-324/09, ECLI:EU:C:2011:474, par. 113 (*L'Oréal and others v. eBay*).

[16] Moreover, such duties may be in conflict with Article 15 of the E-Commerce Directive, which prohibits general monitoring duties.

down rules themselves, or who may promote self-regulatory efforts.[17] In the Netherlands, there are no formal rules regarding notice-and-take down in place. Nor does Dutch law obligate the implementation of such mechanisms. However, in one instance, a Dutch Court of Appeals ordered an intermediary to implement a notice-and-take down mechanism on the basis of Article 26d of the Dutch Copyright Act, which enables courts to issue injunctions against intermediaries whose services are used for infringements.[18]

The *Nationale Infrastructuur ter bestrijding van Cybercrime* (NICC – National Infrastructure to fight Cybercrime), the Dutch government, businesses and interest groups have created a voluntary code of conduct on 'notice and take down'.[19] This code is currently administered by ECP, which is an independent platform for businesses, Dutch government organizations, and interest groups, and aims to foster the use of information technologies in the Dutch society.[20] There is no formal list of members adhering to the code of conduct. Parties that are known by the ECP to endorse the code of conduct are listed on ECP's website.[21] For example, the code has been endorsed by internet access provider KPN, the Dutch Hosting Service Provider Association, NLKabel (an association of cable network providers), and service providers such as Google and Marktplaats/eBay. In addition, Brein, which represents the entertainment industry and the anti-counterfeiting organization, SNB-react, both endorse the code. The Dutch civil liberties organization Bits of Freedom also participated in the setting up of the code of conduct,[22] but is not listed as a party that supports the code.

The code of conduct applies generally to any kind of unlawful information or conduct. It establishes a procedure for intermediaries to deal with notifications of unlawful online information. The code of conduct applies to any kind of unlawful online information or activities. This system mixes elements of notice-and-*take down* and notice-and-*notice* systems. In essence, the code requires endorsing parties to take down content when it is manifestly unlawful. If it does not consider that the materials are manifestly unlawful, the intermediary is required to inform the person that filed the notice and give an explanation. If the

[17] Article 16(1)(a) of the E-Commerce Directive.

[18] Hof Amsterdam, 19 August 2014, ECLI:NL:GHAMS:2014:3435 (News-Service Europe).

[19] B. Koops, *Cybercrime Legislation in the Netherlands*, *in* Country report for the 18th International Congress on Comparative Law, Washington, DC, 25-31 July 2010, session "Internet Crimes" (2010), p. 31. N.A.N.M. van Eijk et al., Moving towards Balance: A study into duties of care on the Internet University of Amsterdam (2010), p. 51-52. The code is available at: http://www.ecp-epn.nl/sites/default/files/GedragscodeNTD-NL.pdf. An English version is available at: http://www.ecp-epn.nl/sites/default/files/NTD_Gedragscode_Engels.pdf.

[20] See: https://ecp.nl.

[21] For a list of endorsements, see: https://ecp.nl/activiteiten/werkgroep-notice-and-takedown.

[22] Kamerstukken II 2003/04, 28 197, nr. 15, p. 4.

intermediary is not able to assess the lawfulness of the materials, the content provider is informed about the notice and requested to contact the person that filed the notice. These people then need to come to an agreement without the intermediary's involvement.[23]

In the Netherlands, there have been no noticeable attempts at the legislative level to extend the notice-and-take down regime, and to burden intermediaries with greater responsibility for unlawful activities. However, at the level of the EU, there is a clear move towards extending the responsibilities of intermediaries for user-activity. The proposed Directive on Copyright in the Digital Single Market would introduce a duty for intermediaries "that store and provide to the public access to large amounts of works" to implement content identification technologies.[24] And the proposed amendments to the Audiovisual Media Services Directive would bring 'video sharing platforms' within the domain of media regulation.[25] The amendments would give these platforms a responsibility to combat hate speech and prevent dissemination of harmful content to minors.[26] Also in other Member States, new legal duties were introduced for intermediaries that go beyond simple notice-and-take down.[27] In that sense, there seems to be a strong push on behalf of right-holder organisations to argue that notice-and-take down is no longer an appropriate means to protect the rights and interests of those harmed by online content, particularly in the domain of intellectual property and hate and harmful speech. Whether such new responsibilities are appropriate, and if they are compatible with the provisions on intermediary liability in the E-Commerce Directive, is a matter of debate.

In our view, careful attention must be paid to ensuring that a fair balance is achieved between competing fundamental rights, and to aspects of legal certainty and due process as required by Article 52(3) of the EU Charter. In this context, useful academic work has been done to investigate the potential of creating distinct kinds of 'notice and action' measures for different kinds of potentially unlawful content (i.e. notice-and-notice for infringement of intellectual property rights, notice-wait-and-take down for defamation; and notice-and-take

[23] Article 6 of the Code of Conduct.

[24] Commission Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market, COM 2016/593. See Article 13 of this proposal.

[25] Commission Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, COM(2016)287.

[26] Article 28a of the proposal.

[27] E.g.: German Bundestag, 'Bundestag beschließt Gesetz gegen strafbare Inhalte im Internet', http://www.bundestag.de/dokumente/textarchiv/2017/kw26-de-netzwerkdurchsetzungsgesetz/513398.

down, combined with occasional notice-and-suspension, for hate speech.).[28] This nuanced, compromise approach takes into account the differences in the seriousness of (alleged) interferences with fundamental rights caused by online speech, and the ease with which breaches can be verified by intermediaries.

Question 1.1.4.

In line with the E-Commerce Directive,[29] Article 6:196c(5) DCC leaves open the possibility of injunctions against intermediaries. It does not, however, constitute a legal grounds upon which such an injunction can be based. Injunctions can be based either on the general duty of care in Dutch tort law ("*onrechtmatige daad*", Article 6:162 DCC),[30] or other specific legal provisions. An example of such a specific provision is Article 26d of the Dutch Copyright Act, which permits courts to order intermediaries whose services are used for infringements to stop providing their service.[31] This basis for injunctions has given rise to some case law in the Netherlands. In particular, on the basis of this provision, Dutch courts have ordered hosting providers to remove websites containing copyright-infringing materials.[32] Injunctions to block access to a particular infringing website may also potentially be based on this provision. In a case about whether access providers could be ordered to block their customers from accessing the Pirate Bay website, the Dutch Supreme Court referred questions to the CJEU on whether that website was infringing and, if not, whether Article 26d might still provide sufficient legal grounds for a blocking order.[33] The CJEU recently ruled that the Pirate Bay was a directly infringing website, thereby allowing it to pass on the second question of whether (and, if so, on what grounds and under what circumstances) a national court could order access providers to block access to a website that is not infringing but which does encourage or facilitate infringement.[34]

A major difficulty with the current EU legislative framework is that it doesn't specify the conditions under which injunctions must be issued. The framework only sets the outer boundaries within which injunctions may be issued.[35] The requirements set out in the EU framework (e.g. Article 8(3) of the Copyright

[28] E.g. C. Angelopoulos & S. Smet (2016). 'Notice-and-fair-balance: how to reach a compromise between fundamental rights in European intermediary liability'., Journal of Media Law, 2016-8 (2), 266-301.

[29] Articles 12(3), 13(2), and 14(3) of the E Commerce Directive.

[30] E.g.: Court of Appeal Den Haag, 15 November 2010, ECLI:NL:GHSGR:2010:BO3980 (*FTD*), par. 5.9.

[31] This provision implements Article 8(3) of the Copyright Directive.

[32] E.g.: Rb. Den Haag, 17 August 2016, ECLI:NL:RBDHA:2016:9685 (*Global Layer*).

[33] HR 13 November 2015, ECLI:NL:HR:2015:3307 (*Brein/Ziggo & XS4ALL*).

[34] CJEU 14 June 2017, case C-610/15 (Brein/Ziggo).

[35] E.g.: Article 15 of the E-Commerce Directive, which prohibits general obligations to monitor; and Article 8(1) of the Copyright Directive which requires that injunctions must be "effective, proportionate and dissuasive."

Directive and Articles 9 and 11 of the IP Enforcement Directive) are very open and leave a lot of room for interpretation and discussion at the Member State level. Dutch legislation implementing these vague rules equally fail to add any additional conditions, procedures, limitations or safeguards that might allow for a more predictable balancing of the relevant competing fundamental rights (e.g. freedom of expression, privacy, intellectual property, freedom to conduct a business). Recent discussions before the Dutch courts on the extent to which the blocking of a website must be effective, and how that effectiveness must be assessed, are merely one example of this.[36] It remains to be seen, moreover, how the procedural safeguards demanded by the CJEU in *Telekabel Wien* as a fundamental prerequisite for any blocking measure might be implemented in practice: Dutch civil procedure does not easily enable intermediaries to test whether a particular mechanism implementing a blocking order would be sufficiently effective to avoid incurring penalties; nor does it easily allow (groups of) consumers to challenge that same mechanism for being excessively effective i.e. for also blocking legal content.

Given the absence of detail in the legislation at both EU and national level, rules on what types of injunctive relief are available, in what kinds of cases and under what conditions, must necessarily be contested in individual court cases. These are decided in first instance at Member State level, and occasionally tested by the CJEU for their compatibility with EU law, including with the fundamental rights protected in the EU Charter of Fundamental Rights. This process of finding appropriate injunctions and their modalities is a time-consuming process. The Dutch proceedings with regard to duty of access providers to block The Pirate Bay are illustrative: proceedings started in 2010 and, as of writing, have not yet come to a final conclusion.[37]

Another type of injunction that has regularly been considered by Dutch courts is the provision by intermediaries of information about customers who have allegedly used their services to disseminate unlawful content. In a landmark decision from 2005, the Dutch Supreme Court held that a hosting provider could be ordered to disclose user data if it was: (a) sufficiently likely that the hosted information was unlawful and damaging to the claimant; (b) the claimant had a sufficiently clear interest in obtaining the user data; (c) no less invasive means to obtain the user data were available; and (d) the claimant's interests outweighed those of the provider and the user.[38] Although the Supreme Court explicitly limited this rule to the issue of obtaining name and address details from hosting

[36] HR 13 November 2015, ECLI:NL:HR:2015:3307, par. 4.3 (*Brein/Ziggo & XS4ALL*).
[37] Rb. Den Haag 11 January 2012, ECLI:NL:RBSGR:2012:BV0549, par. 1 (*Brein/Ziggo & XS4ALL*).
[38] HR 25 November 2005, ECLI:NL:HR:2005:AU4019 (Lycos/Pessers).

providers, the same criteria have subsequently been used to order the provision of other kinds of information and from other kinds of intermediaries.

One of the more pressing issues when applying these criteria, also in the light of the CJEU's decision in *Bonnier Audio*, is the extent to which the claimant demanding identifying information must provide clear evidence that the user has indeed acted unlawfully.[39] This is generally difficult for the intermediary to assess without involving the user in the proceedings, yet Dutch civil procedure does not provide for a procedure similar to US John Doe proceedings, in which an anonymous person can appear in proceedings to defend his right to maintain anonymity.[40] An innovative approach to this conundrum was provided by the District Court of The Hague, which awarded an order to disclose user data that was suspended for two weeks to enable the user to provide a reasoned objection to the intermediary, which could then be assessed by the court. The court duly considered the user's anonymously provided objections, and ruled in the claimant's favour.[41]

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.

The main difficulties lie in the question of how the remedies of repair and replacement relate to the right to termination (and price reduction). Can the consumer already terminate the contract when repair is not possible, but replacement is (or vice versa); or is the consumer then required to choose for the remedy that is available? This matter is not really addressed in case-law or literature. Secondly, it is unknown whether, in case of termination, the seller may require compensation for the loss in value of the goods that occurred during the period in which the defect had not yet manifested. If not, then the consumer may have used the goods for a long time without having to pay anything to the seller, solely because the lack of conformity did not become apparent until a later stage.[42] This is particularly relevant since under Dutch law, as opposed to the Consumer Sales Directive, a remedy for lack of conformity could arise many years after delivery, as the time limit on the right to claim a remedy is 20 years after delivery, or 2 years after notification of the defect.

[39] CJEU 19 April 2012, case C-461/10, par. 56-60.

[40] N. Gleicher, 'John Doe Subpoenas: Toward a Consistent Legal Standard', 118 The Yale Law Journal 320.

[41] Rb. Den Haag 5 October 2015, ECLI:NL:RBDHA:2015:11408; Rb. Den Haag 6 November 2015, ECLI:NL:RBDHA:2015:12706.

[42] See M.B.M. Loos, *Consumentenkoop*, Monografieën BW B-65b, third edition, 2014, no. 37, with references.

Question 1.2.2.

This question cannot be answered in the abstract. The proposal certainly contains good provisions, but also questionable aspects. The application of the rules to contracts for the supply of 'gratuitous' digital content are controversial, in particular as the proposal makes use of the notion of 'counter-performance' by way of the supply of personal data. While it is a good thing that such contracts are covered by the proposal, the fact that it would not apply if the information is not provided *actively* by the consumer (but instead gathered secretively through cookies by the supplier) is not to be welcomed.[43] In addition, the primacy of subjective over objective conformity criteria should be abolished,[44] and the remedies for failure to supply should be clarified (since only termination and – under very strict conditions – damages are mentioned, the question arises whether consumers may also demand specific performance).[45] The remedies for lack of conformity also need to be amended. In particular, the consequences of termination are not yet properly developed and the right to damages is too restricted without an explicit reference to national law that allows for additional possibilities to claim damages.[46]

Question 1.2.3.

This proposal is much more controversial. First, the limitation to online and other distance contracts is unworkable in practice. It seems therefore likely that

[43] See M.B.M. Loos, Not good but certainly content. The proposals for European harmonisation of online and distance selling of goods and the supply of digital content, in: I. Claeys and E. Terryn (eds.), *Digital contracts*, Cambridge: Intersentia, 2017, p. 3-53 (p. 29); H. Beale , Scope of application and general approach of the new rules for contracts in the digital environment, In-Depth Analysis , Briefi ng note for the Legal Aff airs Committee of the European Parliament, PE 536.493 , 2016 (available at: http://www.europarl.europa.eu/committees/nl/events-workshops.html?id=20160217CHE00181, last visited on 15 March 2017), p. 13; V. Mak , The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content. In-depth analysis, Briefing note for the Legal Affairs Committee of the European Parliament, PE 536.495 , 2016 , (available at http://www.europarl.europa.eu/committees/nl/events-workshops.html?id=20160217CHE00181, last visited on 15 March 2017), p. 9.

[44] Beale 2016, pp. 20- 21; Mak 2016, p. 15; R. Mańko, Contracts for supply of digital content. A legal analysis of the Commission ' s directive proposal. In-depth analysis, May 2016 (available at http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA(2016)582048, last visited on 15 March 2017), pp. 22-23.

[45] Loos 2017, p. 35.

[46] Loos 2017, p. 42-46; Mak 2016, p. 15; B. Fauvarque-Cosson , The new proposal for harmonised rules for certain aspects concerning contracts for the supply of digital content (termination, modification of the digital content and right to terminate long term contracts), In-Depth Analysis, Briefing note for the Legal Affairs Committee of the European Parliament, PE 536.495 , 2016 (available at: http://www.europarl.europa.eu/committees/nl/events-workshops.html?id=20160217CHE00181, last visited on 15 March 2017), p. 7.

Member States will only agree to adopt the proposal for an Online Sales Directive if its scope is enlarged to include also on- and off-premises contracts.[47] This would mean that the proposed Directive would ultimately completely replace the current Consumer Sales Directive. Secondly, the relationship between the proposal and general contract law needs to be clarified, e.g. whether consumers are entitled to damages in case of lack of conformity,[48] and whether a consumer may invoke a defect of consent, such as mistake, under national law.[49] It is a matter of policy what the period should be during which the seller is liable for lack of conformity. The original proposal to have a two-year cut off-period would decrease consumer protection as to the duration of the conformity period in one way or another in 12 Member States.[50] Moreover, from the point of view of sustainability, a longer period seems preferable.[51]

On the other hand, regarding the question of whether a defect already existed at the moment of delivery, the 2 year period during which the burden of proof is shifted (during which the seller remains liable for a lack of conformity) may prove to be too long for Member States and European Parliament.[52] However, if the proposal were to be adopted in the original form on this point, the Directive would lead to a considerable *improvement* of consumer protection in *all* Member States. This could ultimately balance out the decrease in consumer protection arising from the duration of the conformity period mentioned earlier – provided that *both* of the proposed provisions are adopted.

Question 1.2.4.

Since these Directives would replace existing national sales law and the laws applicable to digital content, Member States will not have a choice but to apply

[47] Loos 2017, p. 13-16; J.M. Smits, The new proposal for harmonised rules for the online sales or tangible goods: conformity, lack of conformity and remedies. In-depth analysis, Briefing note for the Legal Affairs Committee of the European Parliament, PE 536,492, 2016 (available at: http://www.europarl.europa.eu/committees/nl/events-workshops.html ?
id = 20160217CHE00181, last visited on 15 March 2017), pp. 7-9. See also Mańko 2016, p. 8-9, in which the at that moment mostly critical views of consumer organisations, industry associations, organisations of legal practitioners and scientists are displayed.

[48] Loos 2017, p. 18.

[49] Loos 2017, p. 18-19.

[50] Loos 2017, p. 20-21.

[51] M. Wendland, Ein neues europäisches Vertragsrecht für den Online-Handel? Die Richtlinienvorschläge der Kommission zu vertragsrechtlichen Aspekten der Bereitstellung digitaler Inhalte und des Online-Warenhandels, *EuZW* 2016, pp. 126-131 (p. 130).

[52] The Online Sales and Distance Sales Directive does not expressly deal with the consumer's right to claim damages for damage caused by the non-conformity. The Explanatory Memorandum to the proposal, p. 3, indicates that this matter is left to national law, but the text of the proposal itself gives reason to question this,

these rules to consumer contracts. Moreover, it is likely that national courts will be required to apply the implementing rules of their own motion, as is the case under the current Consumer Sales Directive[53] and will most likely be the case with regard to all Directives in the area of consumer law.[54] The proposal on goods – in particular, if it ultimately will also apply to off-line contracts – contains considerably more detailed rules than the current Consumer Sales Directive. It is therefore self-evident that more EU consumer protection legislation will be enforced by the national courts.

Question 1.2.5.
These Directives offer a good starting point, but leave many gaps. For instance, most of the existing consumer protection rules apply only where the trader provides goods or services in exchange for money. However, in circumstances where the consumer in fact 'pays' with other means (data or time), the contract is not covered. In addition, where the consumer is the *seller* and the trader is the buyer, again, most Directives do not apply (though the UCTD and possibly also the UCPD is/are the exception(s)). Moreover, the relationship between consumer and platforms is not well regulated (e.g. is the platform the buyer or an intermediary? How are standard contract terms incorporated? How about liabilities?). This is particularly the case when the consumer is the seller.

Question 1.2.6.
Not yet, but a case between the Dutch consumer organization *Consumentenbond* and Samsung is pending.[55] Earlier, a case between a smaller consumer organization, *HCC* and Dell Computers led to the annulment of several unfair contract terms, and furthermore – since Dell ignored an order to no longer use the terms – the action ultimately to a successful claim for a *dwangsom* (French: *astreinte*).[56]

Question 1.2.7.
Absolutely, and for several reasons. First, in contracts with other businesses, a business may still be the weaker party and in need of protection. An example relates to the terms and conditions of Internet Service Providers (ISP). These

[53] CJEU 4 June 2015, Case C-497/13, ECLI:EU:C:2015:357 (Faber).
[54] CJEU 21 April 2016, case C-377/14, ECLI:EU:C:2016:283 (Radlinger/Finway), points 66 and 67.
[55] https://www.consumentenbond.nl/binaries/content/assets/cbhippowebsite/actie-voeren/updaten/dagvaarding-consumentenbond---samsung-11-nov-2016.pdf.
[56] Court of Appeal The Hague 6 July 2004, *NJ* 2004, 483, *TvC* 2005/4, p. 189, case note M.B.M. Loos (HCC/Dell Computer I); Court of Appeal The Hague 22 March 2005, ECLI:NL:GHSGR:2005:AT1762, *TvC* 2005/4, p. 150, case note M.Y. Schaub and M.B.M. Loos (HCC/Dell Computer II); Court of Appeal The Hague 24 October 2006, ECLI:NL:GHSGR:2006:AZ0734, *TvC* 2008/2, p. 76 (Dell Computer/HCC III).

terms allow the ISP to claim full payment in case of early termination, and are frequently litigated in the Netherlands on the basis of unfair terms legislation – with differing outcomes.[57]

Secondly, since the Court of Justice defines the notion of consumer very restrictively,[58] there arise many cases where a natural person acts for dual purposes (both as a private person and in the course of a business, e.g. when buying a laptop computer) and does not fall within the protection of EU consumer law. If the scope of consumer protection rules were to be enlarged to also include such contracts, these persons would also obtain protection, and this is much needed in our opinion.[59]

1.3. Geo-blocking

Question 1.3.1.

The interlink between the Geo-blocking Regulation and Regulation 1215/2015 for the purposes of determining jurisdiction

The envisaged Geo-blocking Regulation prohibits the blocking of access to online interfaces and the rerouting of customers from one country version to another. When a trader is compliant with the Geo-blocking Regulation, its online interface will be fully and equally accessible by customers from other Member States as well as those from the Member State to which the trader's online interface was originally addressed. The Geo-blocking Regulation stipulates that the trader may not refuse a transaction based on the domicile of customers from these Member States.[60] For the purposes of determining jurisdiction, it is relevant to determine whether this trader is now "directing its activities" to these Member States within the meaning of Article 17 (1) (c) of Regulation 1215/2012.[61]

[57] See Court of Appeal Arnhem-Leeuwarden, location Arnhem, 25 June 2013, ECLI:NL:GHARL:2013:4517; Court of Appeal Arnhem-Leeuwarden, location Arnhem, 4 August 2015, ECLI:NL:GHARL:2015:5803; Court of Appeal Arnhem-Leeuwarden, location Arnhem, 27 October 2015, ECLI:NL:GHARL:2015:8057; Court of Appeal Arnhem-Leeuwarden, location Arnhem, 24 May 2016, ECLI:NL:GHARL:2016:4014; Court of Appeal Arnhem-Leeuwarden, location Arnhem, 31 May 2016, ECLI:NL:GHARL:2016:4217; Court of Appeal The Hague 5 July 2016, ECLI:NL:GHDHA:2016:1845; Court of Appeal The Hague 6 September 2016, ECLI:NL:GHDHA:2016:2509; Court of Appeal Arnhem-Leeuwarden, location Arnhem, 15 November 2016, ECLI:NL:GHARL:2016:9109.

[58] CJEU 20 January 2005, case C-464/01, ECLI:EU:C:2005:32 (Gruber/Bay Wa AG).

[59] See already M.B.M. Loos, Consumer sales law in the proposal for a Consumer rights directive, *European Review of Private Law* 2010/1, p. 15-55 (p. 18-19).

[60] For further information on geo-blocking in the e-commerce sector, we would recommend reading the European Commission's findings on geo-blocking in the final report on the e-commerce sector inquiry.

[61] Articles 17 (1) (c) and 18 (1) of Regulation 1215/2012 stipulate that if a consumer contract has been concluded with a person, a trader, who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to the Member State of the consumer's domicile, and the contract falls within the scope of such activities, a consumer may also bring

The Geo-blocking Regulation itself answers this question as follows: the mere fact that a trader acts in accordance with the provisions of this Geo-blocking Regulation should not be construed as implying that a trader directs its activities to the relevant consumer's Member State within the meaning of Article 17 (1) of Regulation 1215/2012 (preamble par. 9-10 and Article 1 (5)). In our view, this means that when a trader is compliant with the Geo-blocking Regulation solely to fulfil its obligations under this Regulation, there is in principle no risk that Article 17 (1) (c) will be triggered (i.e. that a consumer may bring proceedings against the trader in the courts of the Member State where the consumer is domiciled).

We do, however, think that when a trader is being 'compliant plus', i.e. going further than is required under the Geo-blocking Regulation, there can be a debate whether the trader is directing its activities to the Member State where the consumer has its domicile. This is especially the case when, for example, the trader translates its website into the local language of the customer and/or offers delivery to the place of residence of the consumer, which is not required under the Geo-blocking Regulation (according to par. 18 of the preamble). We think that in such circumstances it can be assumed that this trader directs its activities to the consumer's Member State within the meaning of Article 17 (1).

For completeness, please note that in the Joined Cases Pammer (C-585/08) and Alpenhof (C-144/09) (and subsequent case-law) the European Court of Justice has given a (non-exhaustive) list of several matters that may be relevant when determining whether a trader is directing its activities to a Member State. According to the ECJ, all clear expressions of the intention to solicit the custom of that Member State's consumers could be relevant to determine whether a trader is directing its activities to a Member State.

Geo-blocking and online gambling

The concept of targeting and geo-blocking is also relevant in various (regulated) sectors, including online gambling. Geo-blocking in the field of online gambling will not be prohibited under the Geo-blocking Regulation. In particular, Article 1 (3) stipulates that gambling activities are excluded from the scope of the Geo-blocking Regulation.

Until the Dutch bill on remote (online) betting and gambling comes into effect, online gambling is forbidden in the Netherlands. The Gambling Authority is targeting all online gambling operators (and also facilitators) who have a specific and distinct focus on the Dutch market. According to the Dutch Gam-

proceedings against this party in the courts of the place where the consumer is domiciled, regardless of the domicile of the other party.

bling Authority, this specific and distinct focus on the Dutch market can (*inter alia*) be shown by the absence of geo-blocking on Dutch customers.[62]

1.4. Questions related to the collaborative economy (COM(2016)356)

Question 1.4.1.

In the paragraph below some general legal issues presented by regulation of the collaborative economy are illustrated. The subsequent paragraph presents an example of successful cooperation between public authorities and collaborative economy businesses in the development of regulation. Competition issues are then considered under Q1.4.2, market access requirements are summarized under Q1.4.3, while Q1.4.4, Q1.4.5 and Q1.4.6 present some consumer protection issues.

Regarding the general legal issues first, a point of contention in the Netherlands has been how collaborative economy businesses should be qualified under Dutch law and whether (and to what degree) traditional sector-specific regulations, such as the Taxi Act and the Housing Act 2014, apply or should apply to them.[63] Furthermore, the liability of collaborative economy platforms for infringements of regulations by the users of these platforms is also at issue in the Netherlands. For example, Uber has been fined as an accomplice for infringements of the Taxi Act by its drivers.[64] On the other hand, the Dutch government does not consider Uber to be a transport company, but rather an information society service provider, and as such seems to take a slightly more permissive approach to sharing economy platforms such as Uber than certain other Member States.[65]

In contrast to the legal issues presented above, some successful cooperative efforts towards regulation can certainly be noted. Examples of such cooperation

[62] Factsheet enforcement with regard to online gambling (in Dutch): http://www.kansspelautoriteit.nl/publish/pages/4572/factsheet_handhaving_online.pdf.

[63] For example, one author examines the Dutch tool-sharing platform Peerby's terms of use in light of the Dutch law concept of lending and concludes that Peerby's version of lending is more akin to renting and may induce greater than anticipated liability on the part of unsuspecting 'lenders', see R. Koolhoven, 'Kwalificatie en rechtspluralisme in 'de deeleconomie'', *Maandblad voor Vermogensrecht*, nr. 6, 2015. See also the Letter of the Minister of Economic Affairs of 18 December 2015, who points out that most problems with regard to home sharing services arise from the lack of a clear distinction between private and commercial service providers, available at: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2015/12/18/kamerbrief-over-toekomstbestendige-wetgeving-digitale-platforms-en-de-deeleconomie-waaronder-particuliere-verhuur-aan-toeristen/kamerbrief-over-toekomstbestendige-wetgeving-digitale-platforms-en-de-deeleconomie-waaronder-particuliere-verhuur-aan-toeristen.pdf

[64] CBb 8 december 2014, ECLI:NL:CBB:2014:450, 5.4.1.

[65] See Reuters newsbulletin of 25 November 2016, available at: http://www.reuters.com/article/uber-tech-spain-court/uber-in-landmark-e-u-court-battle-to-escape-strict-rules-idUSL1N1DQ0YO.

are so-called 'right to challenge' experiments, in which the public authorities allow collaborative economy businesses to propose alternatives to current regulation. Amsterdam is generally regarded as progressive in its approach to the collaborative economy and has even been dubbed a 'sharing city' for its willingness to work with various collaborative economy platforms. Most notably, the city of Amsterdam entered into a Memorandum of Understanding ("**MoU**") with AirBnB, setting out common goals and rules aimed at curbing the negative effects on neighbourhoods of permanent commercial renting of apartments using AirBnB. For example, the MoU contains a rule that apartments may only be rented out for a maximum of 60 days per year.[66]

Question 1.4.2.

In the Netherlands, unfair competition concerns have been voiced – by advocates and associations for traditional service providers – that collaborative economy businesses have an unfair advantage vis-a-vis regulated traditional service providers. Some authors point out that home cooks selling meals via AirDnD for profit are not subject to inspections by the Food and Consumer Product Safety Authority, while traditional restaurant businesses are. Moreover, they point out that inhabitants who rent their apartment using AirBnB, Wimdu or Booking.com are not subject to the plethora of regulations that hotels have to comply with. Finally, they point to ride-sharing service providers such as Uber, Lyft and BlaBlacar who are operating without a taxi license, putting licensed taxi drivers at a disadvantage.[67]

Competitions concerns related to collaborative economy businesses were addressed by a Dutch court in Uber's appeal for an injunction against enforcement of the Taxi Act's licensing requirement against Uber and its drivers in 2014. In this case, Uber argued that a ban on UberPOP served to shield the licensed taxi industry from competition and was therefore contrary to the Regulation's goals of undistorted competition in fair and open markets to increase consumer protection, freedom of choice and best value for consumers.[68] The court however ruled that the taxi licensing system was a legitimate form of market organisation and protecting licensees from unlicensed competition was inherent to such a system. [69]

[66] Memorandum of Understanding between city of Amsterdam and AirBnB available at: https://www.amsterdam.nl/publish/pages/813509/agreement_amsterdam_and_airbnb_mou.pdf. As testimony to the success of this cooperation, the European Commission considers the MoU to be a 'best practice' in developing an EU-wide model contract for use by municipal authorities and home sharing services.

[67] S. Ranchordas 2016, 'regels voor de digitale deeleconomie, oftewel 'uber-regulering', RegelMaat, 2016 (2).

[68] CBb 8 december 2014, ECLI:NL:CBB:2014:450, 5.7.

[69] CBb 8 december 2014, ECLI:NL:CBB:2014:450, 5.7.1.

Question 1.4.3.
Possibly the three most relevant sets of market access requirements in the Netherlands for collaborative economy service providers are the licensing requirements for passenger transportation providers, for apartment renters and for (alcohol serving) hospitality industry operators, as they may be applicable to ride-sharing service providers, apartment-sharing service providers and meal-sharing service providers respectively.

All those who transport people by car for a reward, but not as public transport, are required to obtain a taxi license under the Taxi Act. The requirements for a taxi license are contained in the Passenger Transport Decree 2000, and include a requirement of trustworthiness (to be demonstrated by a so-called declaration of good behaviour) as well as a requirement of skill (to be demonstrated by the completion of training for taxi drivers).

Second, a license is required to be able to use apartments with a permanent housing designation for purposes other than housing, such as renting them out for use as tourist accommodations. The Housing Act 2014 prohibits taking apartments – in buildings designated as housing – out of the 'housing supply' by using it for other purposes than permanent residence without a license from the city council. For example, the city of Amsterdam has designated most apartments as housing and has a broad discretion to refuse licenses which take apartments out of the housing supply. Enforcement of this licensing requirement has resulted in fines for homeowners who are held responsible for the renting of their apartments on AirBnB, even if their tenants were sub-letting the apartment.[70]

Finally, a license is required to serve drinks in a venue by trade or as a business according to the Licensing and Catering Act 2013. The requirements for a license to operate a hospitality business are contained in the Licensing and Catering Decree, and include *inter alia* requirements concerning the 'social hygiene' of the venue and of persons in charge of the venue as well as a screening of the applicant for the potential danger of use of the venue for money laundering or other criminal acts under the Public Administration Probity Screening Act.

Question 1.4.4.
To the knowledge of the authors, no challenges to collaborative economy businesses have been mounted by consumers based directly on consumer protection provisions. Consumer protection considerations were however at the core of Uber's appeal for an injunction against enforcement of the Taxi Act's licensing requirement against it and its drivers in 2014.[71] In short, Uber argued that its

[70] ECLI:NL:RVS:2017:649.
[71] ECLI:NL:CBB:2014:450.

requirements for drivers guaranteed a sufficient level of consumer protection; so that application of the licensing requirement under the Taxi Act would not be necessary to guarantee the necessary level of protection for its customers. The court however ruled that the fact that a recent bill of health and a specific taxi driver's training course are required in order to obtain a license under the Taxi Act meant that Uber's requirements were not substitutable for the requirements under the Taxi Act.[72] Furthermore, the court ruled that the level of enforcement by Uber of its policies was not up to par with the public enforcement of the licensing requirements, and could therefore not be substituted for public oversight.[73]

Question 1.4.5.
The definition of a trader is any natural or legal person who is acting for purposes relating to his trade, business, craft or profession and anyone acting in the name of or on behalf of a trader. The Dutch Civil Code ("**DCC**") actually contains several, albeit similar, definitions of a trader in provisions implementing the different EU Directives for consumer protection. The Consumer Protection Enforcement Act refers to traders as mentioned in:

(i) Directive 2005/29/EC on Unfair Commercial Practices (implemented in section 3A of title 3 of book 6 DCC),
(ii) Directive 2011/83/EU on Consumer Rights (implemented in section 2B of title 5 of book 6 DCC),
(iii) Timeshare Directive 2008/122/EC (implemented in title 1A of book 7 DCC).

The Dutch Government has acknowledged that the frequency of trading, an aim of generating profits and the size of turnover can be criteria to determine whether someone is acting in the capacity of a trader. However, it also warns that the legal definition of a trader should not be unduly limited, and therefore other circumstances may have to be considered on a case-by-case basis. In the same vein, it has acknowledged that it may be difficult to establish thresholds based on generated income, in deciding whether an activity is performed by a trader or not, without considering the particular features and legal context of the market in which the activity at issue is performed.[74] In this regard, see also the answer to Q1.2.7 above.

[72] ECLI:NL:CBB:2014:450, para. 5.6.4.
[73] Ibid.
[74] Letter of the Minister for Foreign Affairs of 8 July 2016, TK 2015-2016, 22112, nr. 2172, available at: https://www.eerstekamer.nl/behandeling/20160708/brief_regering_fiche_een_europese/document3/f=/vk5posimhzzg.pdf.

Question 1.4.6.
A recent study commissioned by the Dutch government on the opportunities and obstacles for innovation in the sharing economy recognizes the value of review systems, and even hints at a role for the government to manage a central review system in order to avoid lock-in effects caused by the fact that reputations are usually non-transferable from one platform to another.[75]

2. Digital Media

Question 2.1.
According to Article 1.1 of the Dutch Media Act, a *programme* ('programma') is an electronic product with visual or media content, that is clearly recognisable and broadcasted as such under a distinctive title via a broadcasting service ('omroepdienst'). A *broadcasting service* ('omroepdienst') is defined as a media service ('mediadienst') that provides media content on the basis of a chronological schedule, which is determined by the institution responsible for the media content, whether or not encrypted by means of a broadcasting channel or broadcasting network, and distributed for simultaneous reception by the general public or a part of the general public. A *media service* is a service that provides media content via public electronic communication networks, for which the supplier has editorial responsibility. As follows from the foregoing, to be qualified as a programme, it is required that the media content is distributed via a broadcasting service, and that the content is received simultaneously by the general public or a part of it. Therefore, according to Dutch law, videos as defined in the judgement would not qualify as a programme. They would however qualify as a media service (on-demand) and therefore fall within the scope of regulation. Since the result of this classification will be that audio-visual material is covered by the Directive and will therefore be governed by the same set of rules, the judgement has not lead to a different approach and will presumably not do so.

Question 2.2.
In the light of the increasing importance of video platforms, resulting in convergence with traditional media, and the role that these platforms play in society, bringing video platforms under the scope of the AVMS may be considered a necessary next step.

Under Dutch legislation, only media services are regulated. A key element in the definition of media services is editorial responsibility. The concept of editor-

[75] ShareNL, 'Innoveren in de deeleconomie', 2015, p. 24-25, available at: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2015/11/01/innoveren-in-de-deeleconomie/innoveren-in-de-deeleconomie.pdf.

ial responsibility is defined in Article 1.1 Dutch Media Act 2008. According to this definition, editorial responsibility means effective control over the choice of media content and the organisation of the media content in a chronological schedule (for programmes) or in a catalogue (for media services on-demand). As most video platforms do not work within such a system of editorial responsibility, they are not regulated.

However, if a system of editorial responsibility does apply, a video platform will be considered a media service on-demand ('commerciële mediadienst op aanvraag') and will therefore be regulated by the applicable provisions in the Dutch Media Act 2008. This includes rules on product placement and the protection of minors against harmful content. In Dutch legislation there are no sector-specific rules for audio-visual platforms. One of the priorities of the Dutch Media Authority in 2017 is the online domain and new ways of access to media content. Therefore, the Dutch Media Authority will focus on the registration on media services on-demand, protection of minors against (seriously) harmful content ('ernstige schade'), surreptitious audio-visual commercial communication ('sluikreclame'), unlawful product placement and other forms of hidden commercial influencing.[76] Moreover, the Dutch Media Authority advocates the regulation of online media in the new AVMS Directive and, until this Directive is implemented in Dutch legislation, is seeking to stimulate initiatives of self-regulation in the online field. .Nonetheless, at this time, there are no sector-specific rules under Dutch legislation.

Question 2.3.

Before answering this question, we would like to refer to the jurisprudence developed in the eighties regarding the Netherlands and its regulation of advertising in broadcasts from other countries. In Case 352/85 (Bond van Adverteerders), the CJEU ruled that the act of broadcasting from one country to the national audience of another country constitutes a transnational service, involving both the service of broadcasting and the service of advertising and that national barriers may only apply – without interfering with the freedom of providing services – under strict conditions. In Case 353/89 (Commission v. Netherlands) it was pointed out that certain conditions on the broadcasting of advertising in television programs from other states may infringe the freedom of providing services in the Treaty.[77]

[76] Commissariaat voor de Media, 'Toezichtbrief 2017: Het nieuwe kijken en het huis op orde', para. 9-14, . 24 November 2016.

[77] ECJ, 26 April 1988, C-352/85 (Bond van Adverteerders), 26 April 1988; C-353/89, Commission v. The Netherlands, 25 July 1991.

In the Netherlands, jurisdiction over broadcasts from other countries is regulated by Article 1.2 Dutch Media Act 2008, referring to Article 2 AVMS. Disputes concerning the jurisdiction of the Dutch Media Authority arose in 2001[78] and 2003[79] and, therefore, under the "Television without Frontiers" Directive 98/552/EEC .[80]

Both decisions concerned a dispute between the Dutch Media Authority and HMG, that broadcasts the Dutch TV-channels RTL4 and RTL5. The official seat of HMG was in Luxembourg, the editorial policy decisions of the board of directors were taken in Luxembourg and RTL4 and RTL5 were being broadcast under a Luxembourg license. On the basis of Article 2 of the Television without Frontiers Directive ("the Directive"), the Dutch Media Authority nevertheless considered that it had jurisdiction over the TV-channels as they fell within the scope of the Dutch Media Act. According to the Dutch Media Authority, HMG was the broadcasting organisation that was responsible for the broadcasting of the channels and, since it had its centre of activities in the Netherlands, most of the HMG-staff involved in the TV-activities were based in the Netherlands. Furthermore, the actual editorial decisions were taken in the Netherlands. Moreover, most of the HMG personnel involved in the pursuit of television activities were based in the Netherlands. Therefore, according to the Media Authority, the provisions of the Dutch Media Act would apply to *RTL4* and *RTL5.*

In its 2001-decision, the highest Dutch administrative court ruled that the Dutch Media Authority was right to assume jurisdiction. However, this would result in double jurisdiction, since the Luxembourg Media Authority also claimed jurisdiction in circumstances where the Dutch Media Authority did not sufficiently comply with its obligation to prevent such cross-overs. Therefore the court overruled the decision.

In 2002, the Dutch Media Authority claimed jurisdiction again, after having discussed the topic in the Contact Committee. However, Luxembourg did not want to give up jurisdiction and the case was brought to court again. The court annulled the decision of the Dutch Media Authority in 2003 on the grounds that it would not be compliant with the Directive and the principle of loyalty as laid down in Article 10 EC regarding compliance with the objectives, system and aim of the Treaty and the actions of its institutions.

[78] ABRvS 10 april 2001, ECLI:NL:RVS:2001:AB1451, *Mediaforum* 2001-6, nr. 27.

[79] ABRvS 6 augustus 2003, ECLI:NL:RVS:2003:AI0788, *Mediaforum* 2003-9, nr. 44.

[80] Both cases are dated before the AVMS, The earlier Directive 89/552/EEG first regulated the country of origin in Article 2.

Question 2.4.

Independence of regulators is not only essential to make sure that media actors comply with the rules. It is also fundamental to the protection of the integrity and independence of the media landscape in the European Union. Independence plays a fundamental role in guaranteeing freedom of information. Independence also provides the essential wall between politics and independent media and is hence one of the cornerstones of democracy. Moreover, independency requirements for a media regulator strengthens its position, which enables it to facilitate the implementation process of EU-legislation and therefore catalyse the creation of a single market in this field.

Under Dutch law, the members of the board of the Dutch Media Authority, an autonomous administrative body, are appointed (and under strict criteria also dismissed) by the Minister of Education, Culture and Science.[81] Board members are not allowed to be politically active or to be involved in public administration, nor in the media. Despite the fact that the Minister has the formal power to overrule decisions of the Dutch Media Authority in exceptional cases,[82] this system has never resulted in any problems of undue pressure on media regulators and we consider the *de facto* independence of the Dutch Media Authority to be very high.

Question 2.5.

One of the main objectives of the new AVMS Directive is to ensure a level playing field, in this internet age and given the many new ways of accessing media content. Within the context of the current AVMS Directive, the harmonisation of schemes of self- and (especially) co-regulation have proven to be successful, as can be demonstrated by the effective protection of minors against harmful content. However, one should keep in mind that (regulation of) the media is closely related to a nation's culture. For example, this can bee seen with the classification of content as seriously harmful. Since there is a crucial cultural dimension in the classification of content as harmful or seriously harmful, harmonisation initiatives should leave sufficient space to take cultural differences into account.[83]

The Dutch Media Authority identifies topics of special interest every year in the so-called 'Toezichtbrief' (Regulation Letter) or 'Handhavingsbrief' (Enforcement Letter). In the last three years, these topics have included independence

[81] Art. 12 paragraph 1 Kaderwet Zelfstandige Bestuursorganen. In practice, the other board members are consulted in the selection process of a new member. This has, however, no formal basis in the law.

[82] Art. 7.9 Mediawet 2008.

[83] Madeleine de Cock Buning, 'Private Regulation and Enforcement in the EU: Finding the right balance from a Citizen's perspective', in: M.de Cock Buning, L.Senden (ed.), Private Actors in Regulation (working title), to be published by Hart Publishers 2018.

and transparency (2015), protection of viewers, and anticipating on developing technologies (2016), compliance with broadcasting laws in the online domain (while stimulating self-regulation for the areas in which the media authority does not yet have jurisdiction) and governance and internal control in broadcasting organisations (2017).

Discussion on the levels of harmonisation has further arisen with regard to practical questions, such as must-carry obligations, the qualification of content as seriously harmful, editorial responsibility and public-private partnerships.

Question 2.6.

These developments are highly dependent upon the technological possibilities. Analog television only offered the possibility of one-way traffic. Viewer data was therefore not available for broadcasters. This was also the case at the start of digital television in the Netherlands. In 2011 UPC (a TV-provider) introduced the Horizon-box platform. This set-top-box made it possible to send data back to the broadcaster, which resulted in, for example, the possibility to recommend videos to specific viewers in the on-demand domains of TV-providers. The possibilities to broadcast personalised commercials are being investigated but this has not resulted in any practical initiatives. In its 2016-'Toezichtbrief', the Dutch Media Authority mentioned the increasing fragmentation of the media landscape. As a next step in this trend, the media authority identified 'personalisation' of media offers under the lead of international companies such as Microsoft, Apple, Google, Facebook and Amazon.[84]

In 2016, the Dutch Data Protection Authority (DPA) investigated KPN and Xs4All, both providers of interactive digital television and found that KPN and XS4ALL created TV-ratings for the purpose of market research without the prior consent of their customers, in circumstances where the ratings could still be linked to identifiable customers. The DPA concluded that XS4ALL and KPN did not provide adequate information to their interactive TV customers about how they collect and process personal data about their TV-viewing behaviour and that this data can be linked to a person's behaviour and interests, which would make it interesting for advertising companies to access this data.[85] The two companies have since then redrafted their privacy statements and data is now processed only for technical purposes.

[84] CvdM, 'Toezichtbrief 2016', 22 December 2015, para. 34. < https://www.cvdm.nl/wp-content/uploads/2013/07/Toezichtbrief-2016-Commissariaat-voor-de-Media.pdf

[85] Conclusions Dutch Data Protection Authority [Autoriteit Persoonsgegevens] of the investigation into KPN and XS4ALL digital interactive TV 20 June 2016, Datahttps://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_report_xs4all_kpn.pdf

As television contains an important cross-border element, we consider harmonisation as a desirable next step in the effective protection of citizens against privacy infringements. Therefore, we are in favour of the further harmonisation of the processing of personal data through the new General Data Protection Regulation. The new General Data Protection Regulation will bring further harmonisation to the processing of personal data.[86]

Question 2.7.

This regime is still applicable and is implemented in the Dutch Copyright Act ('Auteurswet') and the Related Rights Act ('Wet op de Naburige Rechten'). The Dutch Copyright Act was amended by the Copyright Contract Act (which entered into force 1 July 2015) with the view to giving the individual authors and performing artists a stronger position in negotiating contracts on copyright transfers with publishers and producers. New technologies and ways of broadcasting content (incl. new platforms) provided authors and performers with additional means of distributing their works, while it became increasingly difficult to negotiate and object against standard provisions in copyright exploitation contracts. The new Copyright Act now contains eight new, non-waivable provisions on exploitation contracts. The main provision is Article 25c which provides a right to 'equitable remuneration'. This remuneration may be reviewed if the exploitation of a work is done in a way that was unforeseen at the time of the initial contract (Article 25c paragraph 6). Additional remuneration may be claimed under the 'bestseller clause', in cases of unexpected success, in Article 25d.[87] The non-use clause Article 25e allows authors to terminate a contract when, after initial acts of exploitation, the copyright holder fails to sufficiently exploit the copyright. In a recent case brought to Court by members of the popular Dutch Band *Golden Earring*, the Dutch Supreme Court (Hoge Raad) found that a copyright contract transferring copyrights can be terminated under Article 25e, but only with a sufficiently serious ground. The court then referred the case to the Court of Appeal for review.[88]

Question 2.8.

In the Netherlands, cross-border portability of digital content may be a problem because of the territoriality of copyright licenses and the business models

[86] The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

[87] P. B. Hugenholtz, Towards Author's Paradise: The new Dutch Act on Authors' Contracts ,in: Liber Amicorum Jan Rosén, G. Karnell, A. Kur, P-J. Nordell, J. Axhamn, S. Carlsson (ed.), eddy.se ab, Visby 2016, p. 397- 407., K. van den Heuvel, 'What does the new Dutch Copyright Contract Law have to offer?', *Kluwer Copyright Blog* 01-2016 < http://kluwercopyrightblog.com/2016/01/13/what-does-the-new-dutch-copyright-contract-law-have-to-offer/>

[88] HR 7 juli 2017, ECLI:NL:HR:2017:1270 (*Nanada c.s. v. Kooymans c.s.*).

of online content service providers. The new Regulation (EU) 2017/1128, which will enter into force after twelve months of publication, will change this.[89] Under the new Regulation, subscribers to portable online content services, which are lawfully provided in their Member State of residence, can access and use those services when temporarily present in a Member State other than their Member State of residence. Consideration 30 of the Regulation states that the Regulation should be interpreted in accordance with Article 7 and 8 of Charter of Fundamental rights and – together with the limited list of means of verification in Article 5 of the Regulation– the means of verification should be read in accordance with the minimisation principle under the GDPR. It is yet to be seen how this will be interpreted when the Regulation enters into force.

3. Digital infrastructures

Question 3.1.

In answer to the first question, the Netherlands has had rules on net neutrality since 1 January 2013, when the Act of 10 May 2012 amending the telecommunications Act (hereafter: "Tw") entered into force.[90] The rules on net neutrality are now contained in Article 7.4a Tw.[91]

As regards the second and third questions, an integrated answer is provided on the basis of the recent judgment by the Rotterdam District Court in *T-Mobile.* In that case, the court found that there is a discrepancy between Regulation (EU) 2015/2120 and Article 7.4a Tw.[92] Article 7.4 Tw explicitly prohibits zero-rating in a third paragraph that reads as follows:[93]

"Providers of internet access services shall not make the charges for access services dependent on the services and applications that are offered or used through these access services"

This categorical ban on zero-rating (hereafter: the ban) was discussed during the parliamentary debates leading to the adoption of the Act of 12 October 2016.[94] Initially, the Netherlands tried to uphold the ban by unsuccessfully vot-

[89] Of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal marketText with EEA relevance,published OJ L 168, 30 June 2017.

[90] The act was published in Stb. 2012, 235.

[91] Following the entry into force of the Act of 12 October 2016 applying the Regulation on net neutrality, Stb. 2016, 409, Article 7.4a has been amended as will be explained below.

[92] ECLI:NL:RBROT:2017:2940. Available at rechtspraak.nl.

[93] Authors translation of 'Aanbieders van internettoegangsdiensten stellen de hoogte van tarieven voor internettoegangsdiensten niet afhankelijk van de diensten of toepassingen die via deze diensten worden aangeboden of gebruikt'.

[94] See fn. 2 above. All parliamentary documents are available at https://zoek.officielebekendmakingen.nl/behandelddossier/34379

ing against the Regulation. The Minister later argued that a closer reading of the Regulation allowed the ban to be upheld.[95] On the basis of this ban, the Netherlands Authority for Consumers and Markets (hereafter ACM), the designated NRA pursuant to the Regulation, took action against the telecommunications provider T-Mobile for offering zero-rating for certain music streaming services.[96]

The ACM, in line with the Minister's position, argued that the Regulation allowed a categorical ban on zero-rating, but this argument was rejected by the District Court.[97] In a nutshell, the Court found no support for the ban in the Regulation; helped in that regard by the fact that an earlier proposal for such a ban by the Netherlands government was rejected by the EU legislature in drafting the Regulation. The judgment further finds that the equal treatment rule applied to *traffic*, rather than the end-user; a conclusion the Court based on reading the first subparagraph, in conjunction with the second and third subparagraph, of Article 3(3) of the Regulation. Pricing modalities such as zero-rating fall, in the opinion of the Court, under the heading of Article 3(1), which contains no categorical prohibition of differentiated prices.

This judgment shows how the Regulation pursues the dual objective of ensuring non-discriminatory treatment of traffic and end-user rights. It may be noted that these two objectives are of a different nature. Traffic exists irrespective of the identity or properties of the parties involved, whereas the end-user rights are inherently connected to the identity of a party connected to the internet. This difference can lead to ambiguity, as the *T-Mobile* case shows. From an end-user perspective, zero-rating is unproblematic because the services used do not impinge on the data limits applicable to a consumer. From the perspective of equal treatment of traffic, the answer is less clear, as zero-rating effectively gives preference to the traffic from the streaming music providers that qualify for the zero-rating. In view of the wide-ranging duty of equal treatment, different treatment between end-users could be argued to be contrary to Article 3(3) of the Regulation. From both perspectives, competitive harm and an impediment to consumer rights could arise, but only in the specific situation whereby, *inter alia*, the provider of internet access services enjoys a degree of market power.[98] However, this requires a case-by-case assessment, such as the one suggested in

[95] This is set out in the Nota naar aanleiding van het verslag. TK 2015-2016 34 379, nr. 6, p. 1, available at: https://zoek.officielebekendmakingen.nl/kst-34379-6.html.

[96] T-Mobile calls this datavrije muziek and it applies to 25 streaming services at this moment, https://www.t-mobile.nl/datavrije-muziek#dienst. In addition, it took action against Tele2 when its terms prohibited customers from tethering their phones, see https://www.acm.nl/nl/publicaties/publicatie/17298/Tele2-past-voorwaarden-op-verzoek-van-ACM-aan/

[97] The core of the reasoning can be found in paragraph 6.5 of the judgment, *supra* fn.4.

[98] In this regard, the analysis continues as an analysis of vertical foreclosure effects.

the BEREC guidelines adopted on the basis of Article 5(3) of the Regulation,[99] and thus would be incompatible with a categorical prohibition. The categorical ban in the Netherlands therefore qualifies as a stricter approach, from the perspective of non-discriminatory traffic management, as it arguably results in a lower level of protection from the perspective of the end-user. In view of its incompatibility with the Regulation, the Act is not applied by ACM, which has coincidentally decided not to appeal the judgment in *T-Mobile*.[100]

Question 3.2.

With regard to the second question, ACM takes measures with regard to the telecommunications sector on the basis of Chapter 6a.1 Tw. This Chapter stipulates that ACM must analyse relevant telecommunications markets as determined in the Commission recommendation on relevant markets susceptible to ex-ante regulation.[101] In its analysis, ACM must consider whether these markets are competitive and whether any companies operating in them have significant market power. If the latter is true, ACM may impose obligations on companies with considerable market power to provide access – at capped prices – for competitors to a wide range of their facilities, including networks, facilities, wholesale services, technical interfaces and protocols.

For example, after a market analysis study, ACM concluded that the market for unbundled access was not competitive and that KPN had significant market power. Consequently, ACM imposed various access requirements and price caps on KPN for the statutory maximum period of three years (at which time ACM has to reconsider its analysis).[102]

As regards to measures implemented by the central government, the Netherlands is well on track to meeting the goal in the Digital Agenda of universal access to internet with speeds of at least 30 Mbps by 2020.[103] In order to meet the goal of universal access to internet with speeds of at least 100 Mbps by 2025, as

[99] Such guidelines have been adopted and are available at http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b_0.pdf.

[100] https://www.acm.nl/nl/publicaties/publicatie/17251/ACM-niet-in-hoger-beroep-tegen-uitspraak-over-netneutraliteit/.

[101] Commission Recommendation of 9 October 2014 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services, OJ 2014, L295/79.

[102] ACM decision 17 December 2015, marktanalyse ontbundelde toegang, available at: https://www.acm.nl/nl/publicaties/publicatie/15087/Marktanalysebesluit-ontbundelde-toegang-2016--2019/

[103] According to the legislative proposal for implementation of the Broadband Directive 2014/61/EU, 97% of Dutch households and 91% of companies had access to 30 Mbps internet, see Kamerstukken II, , 2016-2017, 34739 nr. 3, p.1, available at: https://zoek.officielebekendmakingen.nl/kst-34739-3.html

formulated in the strategy on Connectivity for a European Gigabit Society, the Minister for Economic Affairs has proposed initiatives for sharing knowledge with local governments about state aid for network capacity expanding projects, and about technical subjects related to the expansion of broadband capacity.[104]

Question 3.3.

In the Netherlands, scarce spectrum is usually allocated by auction.[105] The courts in the Netherlands have generally ruled, following challenges to specific governmental decrees by which spectrum was allocated, that regulations concerning spectrum management were not in breach of European legislation.[106] However, the government has recently published its third Radio Spectrum Policy Memorandum – setting out medium-to-long term policy goals – and it remains to be seen whether the resulting initiatives will lead to fresh challenges following future auctions.[107]

Question 3.4.

ACM is the designated NRA for the Dutch telecommunications sector. In the period leading up to the creation of ACM in 2013, one author opined that the institutional structure of the then-future organisation would not satisfy the criteria for independence as laid down in various EU Directives concerning regulated sectors.[108] According to this author, ACM would lack institutional independence from the Ministry of Economic Affairs, *inter alia* because ACM would not possess legal personality, and the ministry would therefore provide its budget and personnel.[109]

[104] Letter from the minister for Economic Affairs to parliament on fast internet in peripheral areas of 16 December 2016, available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2017/07/03/kamerbrief-over-snel-internet-in-het-buitengebied

[105] For example the Multiband (800, 900 and 1800 Mhz) auction of 2012 and the 2.6 Ghz auction of 2010. A press release for the Multiband auction is available at: https://www.agentschaptelecom.nl/sites/default/files/press-release-dutch-frequency-auction.pdf. The Telecommunications Act 3.10 also allows for allocation by contest, but auctions are preferable according to government policy, see also the Radio Spectrum Memorandum Policy 2016, p. 10, available at: https://www.government.nl/documents/reports/2017/03/07/radio-spectrum-policy-memorandum-2016 , and ECLI:NL:RBROT:2002:AE5810.

[106] For example in the Multiband case, ECLI:NL:RBROT:2014:7917, the court ruled that a provision for new entrants in the regulation on the method of auctioning was not in breach of the Authorisation directive 2002/20/EC, the Framework directive 2002/21/EC or state aid law. See also J. Wolswinkel, 'The Allocation of Radio Frequencies in the Netherlands', in: *Scarcity and the State II*, P. Adriaanse et al (eds), Intersentia:2016.

[107] See note 17 above.

[108] Van Eijk, N. (2012). ACM onafhankelijk? Jaarboek – Koninkijke Vereniging voor de Staathuishoudkunde, 2012,
299-230.

[109] With the exception of the regulatory task of ACM with regard to the transport sector, for which the Minister for Infrastructure and Environment is responsible.

Coincidentally, the question of whether ACM should be given distinct legal personality – to have its own personnel and budget – was also raised in this context during the parliamentary debate preceding the creation of ACM.[110] The Minister for Economic Affairs responded that these features where not necessary to satisfy the requirements of independence in the EU Directives. Accordingly, ACM was created as an independent administrative body without its own legal personality, personnel or budget.

With regard to the institutional independence of ACM and its personnel, Dutch law stipulates that personnel that are made available to independent administrative bodies (such as ACM) report exclusively to the independent administrative body concerned.[111] The Act establishing the ACM (*Instellingswet Autoriteit Consument en Markt*) furthermore contains a provision which precludes the Minister from issuing instructions in individual cases to ACM personnel or its board.[112] Therefore, the Minister has no formal involvement e.g. in the market analyses on unbundled access that ACM conducts on a three-yearly basis in the telecommunications sector, as mentioned under Q3.2 above.

With regard to policy, although the Minister for Economic Affairs has the competence to formulate policy for the telecommunication sector, it has been recognized that the Minister must take the requirements of independence for NRA's in the EU Directives into consideration when formulating policy for ACM.[113] As regards to policy formulated by ACM itself, the Minister does not have competence to nullify ACM's policy or legislation with regard to the energy, postal, telecommunications and transport sectors.[114] Although ACM is bound to inform the minister of its intended policy decisions with regard to these sectors, the minister has no right of veto with regard to such decisions.

To the knowledge of the authors, no concerns about ACM's independence have, to date, resulted in legal challenges to ACM's legitimacy as an independent NRA.

4. Data in the digital economy

Question 4.1.

The preparation in the Netherlands for the application of the General Data Protection Regulation (GDPR) takes place at various levels, involving public authorities as well as the private sector.

[110] Kamerstukken II 2011/12, 33186, 3, p. 6-7, available at: https://zoek.officielebekendmakingen.nl/kst-33186-C.html.

[111] Kaderwet zelfstandige bestuursorganen (stb. 2014, 483), art. 16.

[112] Instellingswet Autoriteit Consument en Markt (stb.2013, 102), art. 9. Also see CBb 29 juni 2010, ECLI:NL:CBB:2010:BM9470, in which the Trade and Industry Appeals Tribunal judged that the minister had issued an instruction concerning an individual case.

[113] Kamerstukken II 2011/12, 33186, 3, p. 11, Kamerstukken II 2010/11, 32814, 3, p. 24.

[114] Instellingswet Autoriteit Consument en Markt (stb.2013, 102), art. 10.

The important changes in the European legislative framework of data protection require an overhaul of the national law for data protection (*Wet bescherming persoonsgegevens*), which will be repealed. The main legislative instrument, enabling full application of the GDPR within the national jurisdictional and administrative frameworks, will be the implementing law of the GDPR (*Uitvoeringswet Algemene verordening gegevensbescherming*, hereafter: "the implementing law").[115] On 9 December 2016, a draft of the implementing law was published by the Dutch Ministry of Security and Justice for public consultation, to which the Ministry received many responses.[116] An important and substantial reaction was given by the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, hereafter: "DPA") and was made public on its website.[117]

The GDPR also completely changes the landscape for the national independent supervisory data protection authorities and how they exercise control. Therefore, DPA commissioned a consultancy firm to calculate the consequences of the new regime for data protection in the EU, and for its resources. Sufficient resources are needed to perform its tasks and exercise its powers in accordance with the Articles 57 and 58 GDPR in an independent and effective manner.[118] In its report, the consultants took the view that the new situation is completely different from the former situation. It emphasized the expected growth of the number of complaints, the new requirements for handling complaints, and the significant increase of European cooperation and *ex officio* investigations, which will require more systemic control. It also mentioned the resources which would be needed for new tasks under the GDPR, such as promoting awareness of public and controllers, prior consultation relating to data protection impact assessments, certification and accreditation, and data breaches. It considers that this new reality will require an increase of staff from the current total of 72 to 185-270 staff (depending on the scenario chosen).[119] The national budget for 2018, as presented by the Dutch government in September 2017, provided for an additional annual budget of €7 million, almost doubling the existing budget of DPA.

This contribution further focuses on a few key components of the implementing law.

First, the relationship between the Regulation and national law is addressed in the explanatory memorandum of the proposed implementing law as a lay-

[115] https://www.internetconsultatie.nl/uitvoeringswetavg/details.

[116] https://www.internetconsultatie.nl/uitvoeringswetavg/reacties

[117] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_uitvoeringswet_avg.pdf.

[118] This control is an essential component of the right to data protection, Case C-362/14, Schrems, EU:C:2015:650, at 41.

[119] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_a_dhr_dijkhoff_inzake_aef.pdf.

ered legislative structure. The Dutch government intends to use its margin of manoeuver in a policy-neutral manner; meaning that, where possible, existing national policies should be affected as little as possible. It also intends to limit the introduction of additional national law and not to use all specifications and derogations in the GDPR. The draft law does, however, contain precise provisions on specific categories of data such as biometric data.

Second, as regards to the setting up of DPA and the guarantees of its independence, as a consequence of the complete independence of the data protection authorities,[120] a few provisions of the national framework law for regulatory authorities (*Kaderwet zelfstandige bestuursorganen*) will not be applicable to the DPA. The Minister will not be entitled to give policy guidance to the DPA, nor will he or she have the power to annul its decisions. The responsible minister has these powers in relation to all other regulators in the Netherlands.

The Dutch rules on the appointment of the members of the DPA will not be changed. These persons will be appointed by the King, on a proposal by the Minister. Arguably, this procedure does not fulfil the transparency requirements of Art 53 GDPR.

Third, on the embedding of the DPA into the national administrative law system, the general legislation on administrative law (*Algemene wet bestuursrecht*) contains provisions on the tasks and powers of authorities that need to be reconciled with the long catalogue of tasks and powers in the GDPR.

Fourth, the draft implementing law provides that it applies to the processing of personal data in the context of activities of organisations in the Netherlands. This means that the criterion for applicability is the establishment of an organisation, not whether the fundamental rights of individuals in the Netherlands are affected; for instance, when services are offered on the internet from another Member State. By comparison, the German implementing law[121] takes the opposite view.

The DPA has provided a long and specific advice on the draft implementing law. Some interesting elements are:

- The DPA should have legal personality.
- The Dutch government should refrain from explaining the uniformly-applicable GDPR, apart from explanations which are not obvious.
- The implementing law should not exceed the discretionary powers provided by the GDPR, particularly in relation to biometric and genetic data.

[120] Further read: Hielke Hijmans, The European Union as Guardian of Internet Privacy, Springer 2016, Ch. 7.

[121] https://www.datenschutz-notizen.de/das-deutsche-datenschutzgesetz-wurde-angepasst-die-eu-datenschutz-grundverordnung-kann-kommen-5018053/.

– The implementing law should include rules on the personal data of deceased persons.[122]

Question 4.2.
Businesses (and public bodies) seem increasingly aware of the need to review and adapt their internal processes to comply with the new requirements of the GDPR. Consultancy firms are also now offering a range of IT tools and compliance checklists. One of the challenges for businesses in the Netherlands, however, in preparing for the GDPR, is that the implementing law has not yet been submitted to Parliament (see above under Q4.1). Moreover, other than the advice given by the DPA in relation to the draft law (see above under Q4.1), the available guidance given by the DPA has been limited to a few documents published on its website. An important document was issued on 13 April 2017 and outlines ten steps to help businesses prepare for the GDPR.[123] The authority also gave guidance on various other issues, such as children's on-line data and on policies to be adopted by schools.

Question 4.3.
Big Data is perceived as one of the key issues from a legal point of view. To ensure the proper use of Big Data, along with safeguards for privacy and other fundamental rights, the government requested the Netherlands' Scientific Council for Governent Policy (*Wetenschappelijke Raad voor Regeringsbeleid*, hereafter: "WRR") to advise on the topic 'Big data, privacy and security.' The government's request of 26 May 2014 focused on four key issues:

– Is it possible to draw a clear distinction in privacy and data protection law between access to data, collection of data, and use of data? And if that is possible, should such a distinction in fact be made?
– How can the process of profiling, and data mining, and other techniques of data-analysis be made sufficiently transparent with a view to security without damaging their effectiveness for security policy?
– What does the development of quantum computers mean for the process of data processing and protection (encryption)?
– What is the impact of Big Data on government data management systems, and how can citizens be involved and influence this process?

[122] In accordance with Recital 27 of the GDPR.
[123] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/in_10_stappen_voorbereid_op_de_avg.pdf

On 31 January 2017, the WRR published a policy brief entitled 'Big Data and Security Policies: Serving Security, Protecting Freedom".[124] In this document, which is based on the WRR Report 'Big Data in a Free and Secure Society' (*Big Data in een vrije en veilige samenleving*)[125], the WRR argued that the use of Big Data in the field of security requires a new regulatory framework. The WRR stated in particular that the emphasis in that framework should be on regulating data analysis and use, rather than on intensifying the regulation of data collection. According to the WRR, it is in data analysis and use that the biggest opportunities and risks of Big Data lie and where new rules are required.

As regards to IoT, the Rathenau Instituut, a Dutch research institution specialized in technology and society, issued a report which highlights that IoT will create new opportunities in the sharing economy. [126] For example, the risk of misuse of goods, theft or illegitimate use will diminish when machines can communicate. This report contains a number of specific recommendations, *inter alia*, that the government should clarify the legal status of sharing platforms, that the government could appoint trusted third parties to supervise platforms and that arrangements could be made to ensure that users can have their data ported to other platforms.

Concerning Machine-to-machine generated data, the Authority for Consumers and Markets ("ACM") announced in a press release dated 13 October 2015[127] that it wanted to tighten the monitoring of 097-numbers in light of the mandatory use of this category for mobile data communication such as M-2-M and IoT. ACM found that most mobile communications providers did not provide sufficient information to consumers and business about this number range and highlighted that laptops were still sold with a data-only connection and 06-number, instead of the mandatory 097-numbers. In a press release of 19 June 2017, ACM announced that the pressure on mobile numbers continues to be strong because of new applications.[128]

Recently, members of the Dutch House of Representatives expressed their concern that IoT developments have led to an increased number of poorly protected devices. In light of the risk of cyber-attacks, they requested that the government investigate whether minimum safety requirements could be imposed

[124] https://english.wrr.nl/topics/big-data-privacy-and-security/news/2017/01/31/wrr-policy-brief-on-use-of-big-data-in-the-security-domain

[125] https://www.wrr.nl/publicaties/rapporten/2016/04/28/big-data-in-een-vrije-en-veilige-samenleving

[126] Report published on 30 May 2017, available via https://www.rathenau.nl/nl/publicatie/eerlijk-delen-waarborgen-van-publieke-belangen-de-deeleconomie-en-de-kluseconomie

[127] https://www.telecompaper.com/news/acm-wants-better-monitoring-of-097-numbers--1107446

[128] https://www.acm.nl/en/publications/publication/17355/Pressure-on-mobile-phone-codes-continues-to-be-strong-because-of-new-applications/

and enforced to protect consumers.[129] Subsequently, in Dutch media, the possibility of an 'Internet of Things quality label' was raised.[130]

Concerning automated cars, the government approved the Autonomous Vehicles (Trials) Bill on 24 February 2017, which allows trials for autonomous cars without a driver on board.[131] By removing legal barriers, Infrastructure Minister Melanie Schultz aims to give manufacturers more opportunities to test autonomous vehicles. Under the new bill, the Road Transport Agency (RDW) will decide in advance, in cooperation with the Institute for Road Safety Research (SWOV), the road authority and the police, on permits to test vehicles that are controlled remotely by human operators on public roads. Permits may, for example, stipulate that the manufacturer must implement measures to make other road users aware that the vehicle is remotely controlled. Based on the road tests, the government will decide on whether further regulation is necessary.

Policy debate regarding smart city proposals are ongoing. There are a number of cooperation initiatives between municipalities that aim to define a common strategy.[132] In this context, one of the contentious issues is the use of Wifi-tracking technology in public-private partnerships. In this respect, it can be noted that the DPA imposed an order subject to penalty payments on a company that offered Wifi-tracking in and around shops.[133] In an official investigation, the DPA found that the collection of personal data by means of Wifi-tracking can be necessary for legitimate business interest. However, in this particular case, the DPA found that the necessary guarantees – to protect the interests of data subjects outside the premises of retailers – were not in place. The authority requested, in particular, that adequate information be provided to the public about the fact that they are being registered by way of Wifi-tracking, and being tracked unnoticed via their mobile device.

The DPA also intervened in a project by the municipality of Arnhem and requested that the collection of individual data by means of 'trash disposal cards' (*afvalpas*) be terminated because of its findings that the collection of personal data in this manner is not currently necessary for exercising public tasks.[134] In a press release dated 2 May 2017 regarding this matter, the DPA highlighted the importance of clarifying the purpose of data collection (in, e.g. tax collection), the importance of informing residents about this purpose and about the use of

[129] MotieHijink and Verhoeven, TK 2016-2017, 26 643, nr. 467.

[130] https://www.nrc.nl/nieuws/2016/11/20/d66-wil-keurmerk-voor-beveiliging-iot-apparaten-a1532668

[131] https://www.government.nl/latest/news/2017/02/24/driverless-cars-on-the-roads

[132] http://gsc3.city/files/strategie/NL_Smart_City_Strategie_Executive_Summary.pdf

[133] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-legt-wifi-tracker-bluetrace-last-onderdwangsom-op

[134] https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-gemeente-arnhem-past-afvalsysteem-aan

their data (which must be proportionate) and the need to adequately protect the 'trash disposal cards'.

Question 4.4.

Since the CJEU's decision in the *Google Spain* case, the right to be delisted has been the topic of quite a number of Dutch court cases.[135] The CJEU in *Google Spain* considered in particular the individual's right to data protection and privacy, the public's right to information, and the search engine operator's economic interests.[136] With regard to the search engine's role, the CJEU focused primarily on the processing and dissemination of personal data by the search engine, and its impact on the individual's right to privacy. In contrast, the Dutch courts in a number of cases also considered the search engine's operator right to freedom of information, the important role of search engines in facilitating access to online information, and the need for courts to exercise restraint in imposing restrictions on their activities so as to protect their catalogue function.[137]

One delisting claim has so far made it to the Dutch Supreme Court, filed by a man convicted of attempting to procure the contract-killing of a competing escort boss. In its decision of 24 February 2017, the Supreme Court held that, in delisting cases related to search engines, it follows from the *Google Spain* decision that the right to privacy, as a rule, overrides the interests of the search engine and the interest of internet users searching for information.[138] However, it also restated the rule from *Google Spain* that a data subject only has a right to delisting if the conditions of (the Dutch implementation of) Articles 12(b) and 14(a)(1) of the Privacy Directive are in fact satisfied. As a consequence, there remains a measure of uncertainty about the applicable norm, and the extent to which (and manner in which) the various competing fundamental rights are to be considered in delisting cases.[139]

[135] For an overview of early case law, see: S. Kulk and F.J. Zuiderveen Borgesius, 'Freedom of expression and 'right to be forgotten' cases in the Netherlands after Google Spain', *European Data Protection Law Review* 2015-2, p. 113-125. See also the summary of recent cases included in the Dutch DPA's reports on mediation requests in delisting cases, most recently: *Autoriteit Persoonsgegevens 11 May 2017,* https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/overzicht_bemiddeling_ap_bij_verwijdering_resultaten_zoekmachines_mei_2017.pdf

[136] CJEU 13 May 2014, C-131/12, ECLI:EU:C:2014:317 (Google Spain, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González).

[137] Rb. Amsterdam 24 September 2014, ECLI:NL:RBAMS:2014:6118; Rb. Amsterdam 12 February 2015, ECLI:NL:RBAMS:2015:716; Rb. Amsterdam 24 December 2015, ECLI:NL:RBAMS:2015:9515; Rb. Den Haag 12 January 2017, ECLI:NL:RBDHA:2017:264.

[138] HR 24 February 2017, ECLI:NL:HR:2017:316.

[139] HR 24 February 2017, ECLI:NL:HR:2017:316, par. 3.5.6.

The DPA has acted as a mediator in several cases in which the search engine operator – usually Google – denied a removal request. In 2016 and again in 2017, the DPA published a report on its decisions in these mediation cases; helpfully including brief summaries of the published court decisions in delisting cases.[140] As of May 2017, the DPA had received mediation requests from 155 individuals. This represents about 1% of the people whose removal requests have been denied by a search engine.[141]

In 70 cases, the DPA decided not to mediate – either because the search engine did not clearly violate Dutch data protection law, the facts of the case were unclear, or there were ongoing legal proceedings. In 54 cases, the DPA did attempt to mediate; in 37 of those cases, search results were eventually removed. In 14 cases, Google stood by its decision not to remove the search results.

It is not clear how the right to be delisted relates to the in principle prohibition to process sensitive data and data relating to criminal convictions and offences. *Google Spain* established that a search engine operator processes personal data by indexing, ranking and displaying it on search engine result pages.[142] If such data is sensitive, would the search engine operator then, in principle, be prohibited from processing such data? Lower Dutch courts have given conflicting rulings with respect to the way in which a search engine operator processes sensitive data. In one case, the Hague District court considered the search results (including snippets) rather than the source pages, and determined that these did not contain facts indicative of criminal conduct. On that basis, it concluded that Google had not processed any criminal personal data regarding the data subject.[143] Google, in essence, is not responsible for the processing of data on the pages it links to. The Midden-Nederland District court did not make the same distinction between search results and source pages, but similarly held that the prohibition on processing criminal personal data did not apply because the source publications at issue only contained *allegations* of criminal misconduct, which had not

[140] *Autoriteit Persoonsgegevens*, 25 May 2016; https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/overzicht_bemiddeling_autoriteit_persoonsgegevens_bij_verwijdering_zoekresultaten_google_0.pdf; and *Autoriteit Persoonsgegevens*, 11 May 2017, https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-bemiddelt-52-keer-bij-verwijdering-zoekresultaten-google-en-bing . For an English summary of the most recent report, see https://www.stefankulk.nl/index.php/1770/dutch-dpa-releases-new-data-about-the-right-to-be-forgotten/.

[141] As of 5 July 2017, Google has received just under 33,000 removal requests, regarding more than 117,000 URLs, of which 53,6% was not removed. See: https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en. The statistics for Microsoft's Bing search engine show a rejection rate of 52% for the Netherlands: https://www.microsoft.com/en-us/about/corporate-responsibility/crrr.

[142] CJEU 13 May 2014, C-131/12, ECLI:EU:C:2014:317, par. 28 (Google Spain, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González).

[143] Rb. Den Haag 12 January 2017, ECLI:NL:RBDHA:2017:264.

been investigated by the authorities and which the data subject denied.[144] The Overijssel District Court explicitly held that the contents of the linked-to page should also be part of the analysis and concluded that a search result pointing to a Facebook post about the data subject's court appearance for child sex abuse involved the processing of sensitive personal data that was *per se* prohibited. It also held that a thumbnail of a business photo of the man was sensitive personal data because it revealed his race, but rejected the delisting request on the grounds that he had authorized the photo to be published.[145]

In a recent ruling regarding a delisting request, related to a lawyer's conviction for a knife crime, the Court of Appeals of the Hague held that a search engine operator can potentially rely on the journalistic exemption, and that there is still room to consider the right to freedom of expression if search engine operators process sensitive data. The Court considered par. 85 of *Costeja,* in which the CJEU referred in passing to the journalistic exemption. The Court concluded that in some cases (as the pointed out by the CJEU), the source publication might be able to invoke the journalistic exemption in circumstances where the search engine can not; and that the CJEU could not have intended to categorically exclude the possibility of taking into account freedom of expression in delisting cases relating to special categories of personal data.[146] In considering the freedom of expression, factors – such as the role that the individual plays in public life – may justify sensitive data being processed by the search engine operator, regardless of the prohibition against processing sensitive data.

In the handful of cases where Google has been ordered to delist search results, the order has been restricted to Google Inc.; claims against the local entity, Google Netherlands, have been rejected on the grounds that it is not the data controller and not capable of carrying out a delisting order. There has been some discussion about the extent of a delisting order against Google Inc., in particular the question of whether delisting should be carried out globally. In general, Dutch courts have focused on search results where Google Search is accessed from the Netherlands, or EU versions of Google Search.

[144] Rb. Midden-Nederland 20 February 2017, ECLI:NL:RBMNE:2017:805.
[145] Rb. Overijssel 24 January 2017, ECLI:NL:RBOVE:2017:278, par. 4.16.
[146] Hof Den Haag 23 May 2017, ECLI:NL:GHDHA:2017:1360, par. 5.8 – 5.11.

TABLE OF CONTENTS

INTRODUCTION 7

QUESTIONNAIRE 33

GENERAL REPORT 75

INSTITUTIONAL REPORT 161

NATIONAL REPORTS 207

- AUSTRIA 209
- BELGIUM 231
- CROATIA 267
- CZECH REPUBLIC 285
- ESTONIA 317
- FINLAND 337
- FRANCE 351
- GERMANY 381
- GREECE 409
- HUNGARY 447
- IRELAND 479
- ITALY 505
- MALTA 539
- NORWAY 565
- POLAND 575
- PORTUGAL 639
- ROMANIA 671
- SLOVENIA 691
- SPAIN 733
- SWEDEN 755
- SWITZERLAND 785
- THE NETHERLANDS 813