jipitec

3 | 2017

Volume 8 (2017)
Issue 3 ISSN 2190-3387

Journal of Intellectual Property, Information Technology, and Electronic Commerce Law

www.jipitec.eu

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 8 Issue 3 November 2017
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

Prof. Dr. Thomas Dreier, M. C. J.,
KIT - Karlsruher Institut für Technologie, Zentrum für Angewandte Rechtswissenschaft (ZAR), Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe Germany

Prof. Dr. Axel Metzger, LL. M.,
Humboldt-Universität zu Berlin, Unter den Linden 6, 10099 Berlin

Prof. Dr. Gerald Spindler,
Dipl.-Ökonom, Georg-August-Universität Göttingen, Platz der Göttinger Sieben 6, 37073 Göttingen

Karlsruhe Institute of Technology, Humboldt-Universität zu Berlin and Georg-August-Universität Göttingen are corporations under public law, and represented by their respective presidents.

ISSN 2190-3387

Funded by
DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

Table Of Contents

Special Issue: Intermediary Liability as a Human Rights Issue

Editorial

Intermediary Liability as a Human Rights Issue

by **Martin Husovec***

Recommended citation: Martin Husovec, Editorial: Intermediary Liability as a Human Rights Issue, 8 (2017) JIPITEC 181 para 1.

1 In early summer 2016, a number of scholars from diverse backgrounds met in Tilburg to discuss issues of intermediary liability and human rights.[1] After a few passionate debates - as well as a round of drinks - a general feeling arose that the social issues at stake require a dedicated forum. To keep the momentum, we decided to set up an informal group - 'Intermediary Liability and Human Rights' - to kick-off periodical meetings and, on the kind invitation of Prof. Spindler, to launch a paper symposium with JIPITEC. This dedicated volume presents the fruits of this intellectual exercise. Its goal is to highlight that design of intermediary liability rules and their real-world effects *can* and also *should* be heavily scrutinized from the human rights law point of view. In this sense, Judge Spano's recent article,[2] in which he argues that the existing ECtHR case-law is best understood only as a starting point and of limited precedential value, is a perfect invitation for scholars in this area to join us.[3]

2 To borrow from the band the Scorpions, 'wind of change' is in the air. Despite the fact that intermediary liability rules have been around for some time, the related debates seem to be increasing in intensity. The selection of contributions in this issue illustrates this very well. First of all, impatience of policy makers results in different types of 'ultimatums', such as the Code of Conduct, which are meant to incentivize a change without amending the laws. Second, there are a number of new policy proposals across the globe, which usually try to legally impose more proactive measures and not just wait for the firms to improve things on their own. Third, the courts are becoming increasingly involved in shaping how the environment should look like; the case-law surrounding hyperlinks and website-blocking are perhaps the most salient symbols of this trend. And lastly, human rights law and its community is awakening to the new 'intermediated' realities of the online world.

3 To name just a few recent initiatives and developments. Within the last few years, the European Court of Human Rights received more than a dozen of new cases in the area.[4] The Council of Europe recently conducted a large scale

* Assistant Professor at the Tilburg University (Tilburg Institute for Law, Technology and Society & Tilburg Law and Economics Center).

1 After the Tilburg meeting organized by me and Tilburg Institute for Law, Technology and Society (TILT), the second meeting took place in Amsterdam and was organized by Tarlach McGonagle at the Institute for Information Law (IViR), University of Amsterdam.

2 Robert Spano, 'Intermediary Liability for Online User Comments under the European Convention on Human Rights' (2017) Human Rights Law Review, p. 11-12.

3 Feel free to drop me an email.

4 To mention just intermediary liability cases stricto sensu: ECtHR, K.U. v. Finland (App. no. 2872/02); ECtHR, Yildirim v. Turkey (App. Nr 3111/10); ECtHR, Akdeniz v. Turkey (App. No 25165/94); ECtHR, Cengiz and Others v. Turkey (App. no. 48226/10 and 14027/11); ECtHR, Delfi AS v. Estonia (Application no. 64569/09) – two decisions; ECtHR, Magyar Tartalomszolgáltatók Egyesülete and Index.hu ZRT v. Hungary (Application no. 22947/13); ECtHR, Rolf Anders Daniel Pihl v. Sweden (App. Nr. 74742/14); ECtHR, Payam Tamiz v United Kingdom (App. no. 3877/14) and pending cases of: Kharitonov v Russia (App no. 10795/14); Grigoriy Nikolayevich Kablis v. Russia (App. no. 59663/17); OOO Flavus and others v. Russia (App. No. 12468/15). The list of the related cases is much broader, see - CoE, 'Internet: case-law of the European Court of Human Rights', available at <http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf>.

study regarding filtering and blocking policies in its Member States and is working on a set of political recommendations.[5] The civil society globally launched a discussion about the principles regarding the best governmental practices.[6] Open Society Foundations commissioned a report on the issue of human rights and self-regulation that was masterfully prepared by IViR.[7] The Internet protocol community has just adopted a new tool to respect human rights in the area of Internet standards.[8]

4 A sceptic may wonder, why all this fuss all of a sudden?

5 Balkin convincingly argues[9] that this is due to emerging privatized control of speech by 'new governors'[10] that challenges our existing human rights safe-guards. As also IViR's report highlights, because the entities are private and our human rights 'supervision' only indirect, we are struggling to approach them in the traditional ways. Unlike the government, these gatekeepers are primarily responding not to a process of political accountability, but to (mostly economic) incentives on the market. But if market outcomes are driven only partly by the legal institutions, then governments can be at best 'co-architects of the environment'. What is then a right approach for achieving human-rights compliant outcomes? Can existing doctrines be always relied on? The contributions of this dedicated volume all reflect on and demonstrate this challenge.

6 To begin with, Belli and Sappa provide a high-level discussion of how intermediary liability rules influence enjoyment of fundamental rights. They argue that when intermediaries are held responsible for their users' activities, the foreseeable consequence is an increase on the types and the granularity of restrictions these private entities will introduce and implement, in an attempt to escape any liability. Moreover, they emphasize intermediaries' regulatory role while contractually regulating the content and applications that their users access and share.

7 Frosio argues that we are witnessing the rise of monitoring obligations that are being imposed on online intermediaries around the world. He observes that proactive monitoring and filtering are increasingly finding their way in the legal system as the preferred enforcement strategy through legislation, judicial decisions, as well as private ordering across the entire spectrum of legal areas. He interprets this trend as the death of 'no monitoring obligations'.

8 Kalėda then zooms in at one of such emerging policies that is heavily used in the European Union, namely injunctions against intermediaries. In his contribution, he analyses how the principle of effective judicial protection shapes the enforcement practice of the website blocking. He argues that these novel injunctions are affecting the rights of multiple third parties. As a consequence, we should give more weight to procedural fundamental rights stemming from Article 47 of the Charter. This new perspective has, in his view, several advantages, such as it must be applied by the courts of their own motion and it could lead to the establishment of a minimum procedural standard across the Member States.

9 Kuczerawy in her contribution reviews the possibilities of the existing legal framework from the perspective of freedom of expression. She is also interested in harmonization, but of different kind. She examines to what extent the doctrine of positive obligations, under both the ECHR and the EU Charter, may require the EU legislator to take additional legal measures to protect freedom of expression online, such as by introducing effective procedural safe-guards.

10 And last but not least, Burke and Molitorisova close by looking at the digital freedoms from the perspective of more encompassing user rights to anonymity. They explore the CJEU's recent McFadden judgment and earlier case-law in order to crystalize the CJEU's position on the anonymity of users. They criticize the disproportionately narrow scope of the judicial analysis and identify a number of useful patterns.

11 The contributions thus represent an excellent mix of doctrinal and comparative approaches to the debate. I hope that the reader will enjoy reading them as much as I and JIPITEC's excellent anonymous peer-reviewers enjoyed reviewing them.

Martin Husovec, November 2017

5 See <http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>.

6 See <https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf>.

7 Christina Angelopoulos, Annabel Brody, Wouter Hins, Bernt Hugenholtz, Patrick Leerssen, Thomas Margoni, Tarlach McGonagle, Ot van Daalen and Joris van Hoboken, 'Study of fundamental rights limitations for online enforcement through selfregulation' <http://www.ivir.nl/publicaties/download/1796>.

8 See <https://www.article19.org/resources.php/resource/38939/en/internet-protocol-community-has-a-new-tool-to-respect-human-rights>.

9 Jack Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2017) UC Davis Law Review; Yale Law School, Public Law Research Paper No. 615.

10 Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2017) 131 Harvard Law Review.

The Intermediary Conundrum

Cyber-Regulators, Cyber-Police or Both?

by **Luca Belli and Cristiana Sappa***

Abstract: The design of intermediary liability regimes has crucial impact on Internet users' capability to fully enjoy their human rights. When intermediary are held responsible for their users' activities, the foreseeable consequence is an increase on the types and granularity of restrictions that private entities will implement to escape liability. This article argues that, besides jeopardizing users' rights, this situation can increase costs for both intermediaries and new entrants, while transforming intermediaries in cyber-regulators and cyber-police. As points of control of networks, platforms and a variety of cyberspaces, intermediaries have the possibility to regulate effectively the behavior of users through their terms of service and to enforce such private ordering in an autonomous fashion, through a number of technical measures. In this regard, intermediaries undertake a true role of private regulators, contractually regulating the content and applications that users are allowed to access and share as well as the ways in which their personal data can be collected and processed. Furthermore, intermediaries are regularly asked by public actors to take active steps in order to enforce national legislation, spanning from copyright infringement to privacy, from illegal hate speech to child pornography. The requests for banning specific forms of expression or limiting their circulation may be in the name of the personality rights, such as the reputation of individuals or companies, but also privacy, personal data protection, or, more frequently, Intellectual Property Rights (IPRs). The implementation of such requests may occur by imposing ex ante filters or blocking techniques, aimed at regulating the flow of information, or by imposing ex post removals of data, notably through notice-and-take-down mechanisms. Crucially, such mechanisms may be imbalanced, protecting specific interests while simultaneously discouraging user expression, participation and innovation, and raising costs for private economic initiatives, thus limiting the fundamental freedom of conducting a business. This work adopts a critical approach to analyze the role that many Internet intermediaries have undertaken as cyber-regulators and cyber-police. Subsequently, it discusses the current legal framework on intermediary liability, with particular regard to the case law of the Court of Justice of the European Union.

Keywords: Internet intermediaries; intermediary liability; private ordering; cyber-police; fundamental rights; Internet-users' rights

Recommended citation: Luca Belli and Cristiana Sappa, The Intermediary Conundrum: Cyber-Regulators, Cyber-Police or Both?, 8 (2017) JIPITEC 183 para 1.

A. Introduction: Intermediaries' Private Orderings and Their Impact

1 As the use of the Internet has increased for both personal communication and business purposes, attention is increasingly turning to the role that intermediaries play. In this context, how the intermediary's liability is designed has a crucial impact on Internet users' capacity to fully enjoy his or her human rights. Users may include natural persons, non-commercial users and business users. Indeed, when intermediaries are held responsible for their users' activities, the foreseeable consequence is an increase on the types and the granularity of restrictions these private entities will introduce and

implement in an attempt to escape any liability.

2 Intermediaries effectively become central points of control over a variety of cyberspaces, including electronic networks, platforms and the network of connected "things"[1]. The intermediaries are able to effectively regulate the behaviour of users through their Terms of Service (ToS). The intermediaries enforce their private ordering through several technical measures. In this regard, intermediaries undertake the role of private regulators, enjoying the power of contractually regulating the content and applications that users access and share. This extends to the ways in which the user's personal data is collected and processed. Furthermore, intermediaries are regularly asked by public actors to take active steps to enforce national legislation, spanning from copyright infringement to data retention, from hate speech to child pornography. The requests for banning specific forms of expression or limiting their circulation, may be in the name of personality rights, such as the reputation of individuals or that of companies. It is also about privacy and personal data protection. More frequently than not, it is about enforcing Intellectual Property Rights (IPRs).[2]

3 The implementation of such requests may occur by imposing *ex ante* filters or blocking techniques,[3] aimed at regulating the flow of information. It may also occur by imposing the *ex post* removals of data. This notably happens by means of notice-and-take-down mechanisms.[4] Moreover, the contractual limitations on the basis of which blocking, filtering and removals are implemented may be based on vague and unclear ToS. This makes it particularly difficult, if not impossible, for a regular user to understand the limits imposed on his or her freedom of expression. Therefore, any user may face legal uncertainty and lack the appropriate remedies to seek redress in the event of abusive blocking or removal occurring. In addition, the implementation of *ex ante* filtering seems to be inefficient. It imposes higher costs, while at the same time conflicting with the principle of proportionality.[5] In fact, *ex ante* limitations to the circulation of information may be imbalanced, protecting specific interests while simultaneously discouraging user expression, participation, and innovation. It may additionally have the effect of hampering the freedom to conduct a business,[6] by raising the costs for private economic initiatives.

4 Intermediaries regulate the services they provide through standard contracts, commonly referred to as adhesion contracts or boilerplate contracts. The main feature of any standard contract utilised by any intermediary is that the contract is not the product of a negotiation.[7] On the contrary, the conditions are pre-determined by and expresses the one-sided control of a single party. Over the past few years, this type of contract has become the object of numerous critique.[8] The critique ranges from the unilateral provisions, the almost entire absence of negotiation between the parties, and the quasi-inexistence of the bargaining power of one party that is required to adhere to the terms. Internet users' mere adherence to the ToS imposed by the intermediaries gives rise to a situation where consumers mechanically 'assent' to pre-established contractual regulation. According to the same ToS, the intermediaries may continue to modify the ToS unilaterally.[9] Hence, except for

* Luca Belli is Senior Researcher at the Center for Technology and Society of Fundação Getulio Vargas Law School (Rio de Janeiro) and Associated Researcher at the *Centre de Droit Public Comparé* of Paris 2 University. Cristiana Sappa is Professor of Business Law at Iéseg School of Management (Lille and Paris). This work is the outcome of a common effort and reasoning from the two authors. However, the draft of Section I has to be attributed to Luca Belli, while Cristiana Sappa drafted Section II and III.

1 The evolution of the control position of Internet intermediaries in the context of the Internet of Things cannot be extensively analysed in this paper and will be the object of a further publication.

2 In this regard, as an instance, intermediaries like Google report to be asked to remove well over 100,000 links to alleged copyright infringing material every hour. See Google, *Transparency Report. Requests to remove content due to copyright*, 2016, <https://transparencyreport.google.com/copyright/overview#glance>.

3 For a complete overview of blocking techniques, their efficency and their collateral effects see Internet Society, *Internet Society Perspectives on Internet Content Blocking: An Overview*, March 2017 <https://www.internetsociety.org/sites/default/files/ContentBlockingOverview_20170326_FINAL_0.pdf>.

4 For an overview of such mechanisms, see J. M. Urban - J. Karaganis – B.L. Schofield, *Notice and Takedown in Everyday Practice*, UC Berkeley Public Law Research Paper No. 2755628, 2017, <https://ssrn.com/abstract=2755628>.

5 See *ibid.*; EUCJ, 24 November 2011, C-70/10, case *Scarlett Extended*, *EIPR* 2012, p. 429ff., commented by D. Meale, *SABAM v. Scarlet: of Course Blanket Filtering is Unlawful, but This isn't the End of the Story.*

6 At EU level, article 16 of the EU Charter of Fundamental Rights explicitly enshrines the freedom to conduct a business. See <http://www.europarl.europa.eu/charter/pdf/text_en.pdf>. This provision finds no explicit parallel in international human rights law although the constitutional elements of this right can be found in the freedom to enjoy the right to property and freedom of expression.

7 See the seminal work of O. Prausnitz. *The standardization of commercial contracts in English and continental* law, Sweet & Maxwell, London, 1937.

8 See most notably: M.J. Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law*, Princeton University Press, 2012; N.S. Kim, *Wrap Contracts: Foundations and Ramifications*, Oxford University Press, 2013.

9 A recent study conducted by the Center for Technology and Society at Fundação Getulio Vargas analysed the Terms of Service of 50 online platforms, establishing that only 30% of the analysed platforms explicitly commit to notifying users

the possibility to "take it or leave it", users have no meaningful say about the contractual regulation they are forced to abide by. This context of "contractual authoritarianism",[10] is further exacerbated in the Internet environment. Besides having the power to unilaterally dictate the ToS, intermediaries also enjoy the capability to unilaterally implement their ToS-based private ordering.

5 Although it can be argued that private orderings are not a problem *per se* if users have the possibility to switch to another intermediary, it must be noted that such a possibility can be severely limited. This can be due to lack of competition, user lock-in practices, and the fact that all intermediaries regulate their services via unilaterally established and unilaterally implemented ToS. Furthermore, the potential benefits of switching to other competitors are greatly reduced when all market players include the provisions that are materially the same within their ToS to avoid liability for content shared by or activities carried out by third parties. In this regard, this article argues that intermediaries may enjoy far-reaching powers on the cyberspaces under their control, while the current legislative tendencies seem to encourage the adoption of "voluntary measures",[11] that strengthen the intermediaries' position of "points of control",[12] rather than reducing it.

6 In the first section of this work, we will critically analyse the role that many Internet intermediaries have undertaken as cyber-regulators and cyber-police. To understand this evolution, we will focus on the concepts "regulator" and "police", to subsequently analyse the functions of Internet intermediaries. In the second and third sections, we will discuss the current EU legal framework on intermediary liability, and consider the evolution of the intermediary liability regime, with particular regard to IPRs violations, while stressing how the implementation of such a regime may limit the full enjoyment of Internet users' fundamental rights. Lastly, we draw conclusions, arguing that the regulation and policing of cyberspaces shall conjugate efficiency and due process requirements. The regulation should be grounded on the responsibility of intermediaries to respect users' fundamental rights. Due to the abundance of intermediary liability literature focused on the US system, and to the potentially global impact of the ongoing EU reforms, we will mainly analyse the regime through a European perspective. We aim to bring a fresh approach to the debate.

B. Section I: From Regulators and Police to Cyber-regulators and Cyber-police

7 Intermediaries are not only vital to ensure the well-functioning of the Internet. They also enjoy the privilege of unilaterally defining the private ordering of the cyberspaces that it comprises of. Hence, such entities become key points of control or "chokepoints",[13] with the aim of providing order and enforcing national legislation into portions of the Internet. Indeed, due to the control they exercise on their systems as well as the enormous amount of data they collect and store about users, intermediaries become essential partners of governmental agencies to conduct investigations and enforce the law of the land.[14] Intermediaries define contractual terms to which users have to abide, enjoy the ability to enforce their ToS independently from state-based law-enforcement mechanisms. Intermediaries put in place alternative dispute resolution processes, adjudicate disputes between users, based on the intermediary-defined contractual regulation, which is implemented via technical means.[15] This combination of quasi-normative, quasi-executive and quasi-judicial powers assigns a particularly authoritative position to the intermediaries. It concentrates a remarkable power in their hands. This power may be deployed on the specific cyberspace under the control of the intermediary, be it a platform, an electronic network or even a

about changes in their contracts; 56% have contradictory or vague clauses, for instance, foreseeing that users will be notified only if the ToS changes are considered as "significant" by the platform; while 12% of the platforms state that there will be no notification in the event of contractual changes regardless of their relevance. See <http://tinyurl.com/toshr>.

10 See S. Ghosh, *Against Contractual Authoritarianism*, Southwestern Law School Review. Vol 44, 2014.

11 The utilisation of such measures was introduced in 1998 by section 230 of the U.S. Communications Decency Act. Since the failed negotiations on the Anti-Counterfeiting Trade Agreement (ACTA), an expanding number of governments has been trying to export the "good Samaritan" clause. See Article 27, ACTA proposing an obligation on States to support "cooperative efforts with the business community" to enforce criminal and civil law online, available at <https://edri.org/actafactsheet/>.

12 See *e.g.* J. Zittrain, *Internet Points of Control*, Boston College Law Review, vol. 44, 2003; L. DeNardis. *Internet Points of Control as Global Governance*, CIGI Internet Governance Papers n° 2, August 2013, <https://www.cigionline.org/sites/default/files/no2_3.pdf>.

13 See e.g. A. Robachevsky, C. Runnegar, K. O'Donoghue and M. Ford, *The Danger of the New Internet Choke Points*, The Internet Society, 2014. available at <http://tinyurl.com/y9qwngxl>; N. Tusikov, *Chokepoints: Global Private Regulation on the Internet*, University of California Press, 2016.

14 These aspects are discussed in Section II and III.

15 See L. Belli. *De la gouvernance à la régulation de l'Internet*, Berger-Levrault, Paris, 2016, pp. 202-209; L. Belli - J. Venturini, *Private ordering and the rise of terms of service as cyber-regulation*, Internet Policy Review, 5(4), 2016.

network of connected devices (or "things"). Such amalgamation of power is due to the intermediary's capacity to define and subsequently control the logical architecture of a given application or the hardware on which network infrastructure and connected things, are based.

8 Internet intermediaries concentrate the powers, because they both create the applications, networks and things under their control and regulate their functioning. In doing so they establish the ToS-based private orderings. Conversely, it is interesting to note that national legislators attribute such combination of powers to the administrative agencies that regulate specific issues, such as telecommunications, personal data protection, or medical products. This section analyses the main features of regulators and police in the offline world. Using these features, we are able to draw parallels between the agency of administrative entities and Internet intermediaries in the subsequent sections. Administrative bodies have a positive obligation to protect human rights and to operate transparently, impartially and in the public interest. However, it may be hazardous to delegate such public attributions to Internet intermediaries. The fundamental purpose of the Internet intermediary is to maximise profit in the private interest, with no duty of impartiality, transparency or human rights protection.

9 While the twentieth century witnessed the emergence of the modern administrative state, the twenty-first century is undoubtedly witnessing the digital transformation of the state and the digitisation of social interactions at large. Such a trend is corroborated by the ever-increasing migration of public activities to the online environment. Furthermore, public services are digitised, social networking platforms are emerging and are constantly encouraging online public debate. The aim is to collect the greatest amount of data on users' interactions. This digital evolution has not simply transformed the way individuals communicate with each other and speak to the polity. It has also empowered various intermediaries with the capability to monitor users, constantly collecting data on individuals' behaviour, and to regulate digital interactions. These transformations have clearly demonstrated that Internet intermediaries play a pivotal role in advancing public policy objectives,[16] due to their position of control. For this reason, the legislature and the government has increasingly delegated traditional regulatory and police functions to the intermediaries that design and organise digital environments.

10 Such delegation was traditionally achieved by stimulating "voluntary commitments",[17] to regulate and police in order to avoid liability. More recently it has taken the form of an obligation to police and decide what constitutes unlawful or "harmful" content. Intermediaries have traditionally tried to avoid liability by banning illicit conduct from the cyberspaces under their purview. These bans are enshrined in the ToS and implemented either algorithmically or manually. Manual implementations are conducted by employing individuals who actively monitor users' compliance to the ToS.[18] However, it must be noted that private regulation may be over-restrictive and private enforcement frequently leads to erroneous decisions.[19] This in turn, may result in unduly limiting the fundamental freedoms of individuals. This effect should suggest to legislators that delegation of traditionally public functions to private intermediaries might be a negative trade-off. Recently adopted legislation, such as the German law on Enforcement on Social Networks is telling.[20] It exemplifies the tendency towards "responsibilisation of intermediaries", by increasing their "voluntary" regulation and policing, rather than decreasing the delegation of public functions to private ordering.

11 To understand the tendency towards the transformation of Internet intermediaries into cyber-regulators and cyber-police, we develop a preliminary digression on the role and functions of regulators and police. We explore the intermediary liability regime and will identify similarities between, on the one hand, traditional regulators and police, and on the other hand, intermediaries acting as cyber-regulators and cyber-police.

16 See OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, OECD Publishing, Paris, 2011, <http://dx.doi.org/10.1787/9789264115644-en>.

17 See, for instance, the Code of Conduct on illegal online hate speech, developed by Facebook, Twitter, YouTube and Microsoft, together with the European Commission, which establishes a series of commitments to combat the spread of illegal hate speech online in Europe <http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf>.

18 As an example, in May 2017, Facebook announced the adding of "3,000 people to [Facebook's] community operations team around the world -- on top of the 4,500 we have today -- to review the millions of reports we get every week." See M. Zuckerberg. (3 May 2017). Official announcement. <https://www.facebook.com/zuck/posts/10103695315624661>.

19 For instance, empirical evidence of over-removal is abundant. For an overview of tools and techniques utilised to implement "takedowns" of illicit content, exploring mistakes "made by both "bots" and humans," see Urban, J. M., Karaganis J. and Schofield B. L, *supra,* note 4.

20 The German Parliament adopted the law on 30 June 2017, requiring every "social media" company operating in Germany and having more than 2 million users to remove content that is deemed as illegal by German legislation – and, therefore, to assess the legality of the content – within 24 hours of the notification.

I. Regulatory Agencies and Police in the Offline World

12 Regulation and police are traditionally considered as public functions, performed by bodies operating independently and transparently, and in the public interest. Over the past century, states restructured their organisations, fostering efficiency and ensuring the transition from the welfare state to the regulatory state. In the process, states developed issue-specific regulation and established issue-specific regulatory agencies.[21] On the one hand, the rise of participatory governance processes grounded the legitimacy of administrative regulation on openness to collective wisdom expressed through numerous associative processes that provide inputs and feedback for the development of regulation. At the same time, it constituted the participatory legitimacy of the administrative agency. On the other hand, regulatory agencies have been relying on a variety of tools – of an administrative or private nature – to provide equilibrium to the sectors under their ambit.[22] Notably, the experimentation of new co-regulatory approaches demonstrated the possibility to strike a balance between conflicting interests, in an efficient fashion. For instance, by promoting technical standards or contractual agreements and avoiding burdensome rule-making processes. In this context, it is important to clarify that regulation can be exercised through a variety of tools that may be more effective than traditional public-law tools, such as through courts decisions or through legislation.[23] Hence, self- and co-regulation undertake a complementary function, becoming particularly widespread when state regulation proves to be ineffective and inefficient.[24]

13 The Internet offers a good case study for the inefficiency of public regulation. This is due to the intrinsic geographic and physical limitations of public law that may prove difficult to implement in a transnational and digital environment. It is in this environment that intermediaries such as content and application providers operate. Hence, Internet intermediaries may either be required to apply national legislation as a condition to operate in a given country, or be encouraged to "voluntarily" regulate user behaviour via more efficient private ordering. It is in this context that intermediaries solely define their ToS, and thereby regulate the cyberspaces under their purview, as if they were private regulators.

14 The term "regulator" is generally used to refer to public authorities responsible for monitoring a specific sector. The regulator addresses the conflicting interests of a wide range of stakeholders and establishes an adequate equilibrium in that sector. Regulators are supposed to act in the public interest. They derive their authority from legislative delegation of power that determines the scope of the issues within their purview. The independence of regulatory agencies is the very basis of their legitimacy. In fact, by being independent from the traditional structure that defines administrative organisations, which is based on a hierarchical structure, regulatory entities are supposed to be shielded from the undue influence of both political and economic interests.[25] Such independence makes administrative agencies less easily susceptible to external pressure. This provides the conditions necessary to regulate in the public interest.

15 A further element of legitimacy for regulators is the specificity of their regulation. Indeed, being unable to rely on a democratic mandate, the legitimacy of an administrative body to regulate depends on the legislature's devolution of a portion of sovereignty, but limited to a specified scope and defined sector. Such delegation signifies the willingness to transfer the authority to regulate a given issue from the democratically elected bodies to specifically mandated agencies. This is carried out on the basis that the agencies enjoy the scientific or technical competencies necessary to take decisions about particularly complex topics. The establishment of independent regulatory agencies aim not only at removing the administration from the influence of political and economic power. It also aims at creating efficient decision-making bodies whose decisions are based on scientific considerations.[26] The development of evidence-based regulation, independent of particular interests, is indeed the real *raison d'être* of the regulatory agencies. In turn, the delegation of regulatory power from the legislature represents

21 Regulatory agencies differ from executive agencies. The former are characterised by independence from the administrative hierarchy and by the attribution of regulatory powers, while the latter are usually affiliated to a ministry or department and manage the implementation of specific governmental policies. See K. Datla and R. L. Revesz, *Deconstructing Independent Agencies (and Executive Agencies)*, in Cornell Law Review, vol. 98, no 4, 2012; Conseil d'État. (2012). Les agences: une nouvelle gestion publique? Les rapports du Conseil d'État. <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/124000501.pdf>; L. Belli, *supra*, note 15, pp. 109-114. In this section, we use the terms agency and regulator to refer generally to regulatory agencies.

22 See L. Belli, *supra*, note 15, pp. 101-102.

23 See *ibid.*, pp. 97-129.

24 See P. Trudel, *Les effets juridiques de l'autoréglementation*, RDUS, vol. 19, 1989, p.250.

25 Although the degree of independence as well as the specific positioning within the administrative structure may vary according to the legal system in which a regulator is established. For a complete analysis of the characteristics of regulatory agencies, see Conseil d'État, *supra,* note 21.

26 See A. Supiot, *Du gouvernement par les lois vers la gouvernance par les nombres*, cours dispensé au Collège de France, 31 janv. au 25 avr. 2013 ; L. Belli, *supra*, note 15, pp. 91-97.

the basis of the agencies' legitimacy to perform their functions. In these circumstances, regulators are established as independent, transparent, and legally predictable entities, overseeing sectors characterised by constitutional relevance and high specificity.[27] It is interesting to note that a very similar rationale justifies the European Court of Justice's delegation of regulatory functions to a particular category of Internet intermediaries. This category refers to search engine providers. They are tasked to operate in a manner that strikes a balance between freedom of information and the privacy of individuals' personal data. The Court has indeed affirmed that search engine providers must assess what information may be considered: "... inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed".[28] Subsequently, the providers must de-index such information, in order to provide effective and complete protection to users. This combination of regulatory and executive functions is a characteristic of regulatory agencies.

16 Indeed, in addition to the traditional administrative functions of authorisation and control, regulatory agencies have the power to lay down general rules. The rules are there to help manage their application services and to resolve disputes with a view to effectively discipline the sectors within their competence.[29] In this context, because of the plurality of powers conferred upon them, the regulators represent a genuine "legal oxymoron".[30] The regulatory entities may be empowered to make rules (regulatory power), control their execution (executive function), adjudicate disputes, and pronounce administrative sanctions (judicial power). The aim is to promote the public interest and to achieve their regulatory objectives effectively. The achievement of a superior – usually constitutional – interest is therefore the rationale that explains the combination of quasi-normative, quasi-executive, and quasi-judicial attributions. Such a combination is justified since the agencies' sector-specific regulation is not politically driven but rather based on objective scientific considerations and empirically demonstrable evidence.

17 Lastly, it is important to stress that some administrative agencies exercise the powers that may be categorised as "special police" attributions. A telling example in this instance may be found in the French Health Products Safety Agency[31] (ANSM), which enjoys the power to inspect industrial sites, conduct controls of laboratories, and conduct scientific, medical or economic evaluations of any product it deems necessary to protect public health. To implement such powers, the agency can take evidence-based decisions to suspend, ban, or restrict the circulation and use of any product or practice that may cause danger to public health. The special police functions performed by ANSM usefully exemplify a distinction between administrative police and judiciary police, which is particularly evident in French administrative jurisprudence.[32] A brief analysis of such a distinction will allow us to better understand the role undertaken by Internet intermediaries that police the cyberspaces.

18 The term "police" generally refers to bodies whose fundamental purpose is to preserve public order and public safety through the enforcement of rules and by assisting the public. On the one hand, administrative policing presents a preventive character, having the main objective of protecting public order and morality,[33] which is unique to every country and may also be structured in special administrative police, dealing with specific issues. On the other hand, judicial policing has a repressive character, aimed at recording offenses against criminal law, gathering evidence and searching for the perpetrators of specific offences.[34] The

27 Positive theories of regulation affirm that regulators are instituted when: the government deems it necessary to protect consumers from potentially abusive behaviours of market players when competition is ineffective or inexistent; to overcome information asymmetries in a given sector while promoting the public interest; to foster competition in a given sector; or to protect specific fundamental rights. An example in this regard is the establishment of the French Data Protection Regulator in 1979, and the subsequent requirement of national data protection authorities for all signatories of the 1981 Council of Europe convention on the protection of personal data. See *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,* available at <http://tinyurl.com/hfowpyp>; Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 1981, available at <https://rm.coe.int/1680078b37>.

28 EUCJ case Google Spain v. Costeja, 14/EN WP 225 of 26 November 2014, para 93, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf>.

29 See L. Belli, *supra*, note 15, 101-119.

30 See P. Gélard, *Les autorités administratives indépendantes: évaluation d'un objet juridique non identifié*, rapport fait au nom de l'office parlementaire d'évaluation de la législation, AN, no 3166, 2006, p. 22.

31 See Conseil d'État, *supra,* note 21, p.50; *Agence nationale de sécurité du médicament et des produits de santé,* <http://ansm.sante.fr/>.

32 Particularly, see Conseil d'Etat, *Consorts Baud*, 11/05/1951, <http://www.lex-publica.com/data/jurisprudence/baud.pdf>; Tribunal des Conflits, *Dame Nouelek*, 7/06/1951, <http://www.lex-publica.com/data/jurisprudence/noualek.pdf>.

33 States have both the right and obligation to determine their own moral values in whatever form they see fit with the aim of meeting the requirements and needs of their citizens. At the EU level, such principle is particularly evident in EUCJ, Case 34/79, *Henn and Darby* (1979), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61979J0034:EN:HTML>.

34 See Conseil d'Etat, *Consorts Baud*, *cit.*; Tribunal des Conflits, *Dame Nouelek*, *cit.*

criteria to distinguish between administrative and judicial police depends on the intent for which police operations are undertaken. It particularly depends on the existence of a link between a police operation and a criminal offence. Administrative policing is aimed at the general preservation of public order and morality. Judicial policing is aimed at the special repression of given offences. Similarly, intermediaries implementing voluntary measures to remove or disable access to specific content act as administrative police. Intermediaries who retain personal data of criminal offenders or block access to content by complying with court decisions, act as criminal police.

19 Policing, as policymaking and giving justice, are considered as quintessentially public functions. However, it must be noted that policing may be delegated to private bodies, to cope with the deficiencies and limited resources of the public bodies. Private police are funded and operated by non-governmental entities with the aim of enforcing (public or private) rules, fostering order and safety within privately owned spaces that are generally publicly accessible, such as shopping malls or residential compounds. Such spaces are publicly accessible but controlled by private entities that may establish their own "police" as a private service, or subcontracting it. The goal is to safeguard both the well-being of the individuals who have access to and the safety of the business that are hosted in the malls or complexes.[35] Similarly, it can be argued that, cyberspaces may be considered as publicly accessible "spaces" although they are created, maintained, and regulated by private intermediaries that can also act as cyber-police to monitor the implementation of both the ToS and national legislation. Private and public police officers have a similar function. Both seek to guarantee the respect of the established rules and increase safety. Private police however may be more concerned with creating a favourable environment for those who fund them rather than with justice.[36] Such considerations seem particularly relevant to properly understand the consequences of delegating to private intermediaries. The natural behaviour of private intermediaries is profit maximisation rather than the promotion of public welfare. The public welfare task, in this context, is to regulate and police cyberspaces, especially when such environments play a pivotal role as a platform that fosters public debate.

35 See P. Heaton, P. Hunt, J. MacDonald and J. Saunder, *The Short- and Long-Run Effects of Private Law Enforcement: Evidence from University Police*, IZA Discussion Paper No.8800, 2015, <http://ftp.iza.org/dp8800.pdf>.

36 See *idem.*

II. Cyber-regulators and Cyber-police

20 The Internet exacerbates the concentration of powers in the hands of private intermediaries, which retain full control over the systems they conceive, operate and regulate. Such a situation has been compared to a revival of feudalism.[37] The intermediaries enjoy quasi-legislative, quasi-executive and quasi-judicial powers. This is giving rise to a form of private quasi-sovereignty.[38] Similarly to the administrative regulators illustrated above, intermediaries enjoy the power to prescribe rules. However, unlike administrative regulators, intermediaries also enjoy the power to modify their contractual regulation at their own discretion,[39] being subject to no other constraint, other than the more or less stringent limits of their contractual autonomy. This means that the intermediaries' private ordering undertakes a quasi-legislative function,[40] consisting of the ability to define what behaviours and what information is allowed within their cyberspaces. As an instance, application providers may unilaterally define what content is banned from their platform, what and how personal data is collected, and even what personal information is no longer relevant or in the public interest and should be de-listed from search engines.[41] Furthermore, intermediaries enjoy the quasi-executive power to implement their contractual regulation by defining the software and hardware architecture of the cyberspaces under their purview and by implementing their own decisions, such as the removal of content deemed as abusive by the ToS. Lastly, intermediaries enjoy a quasi-judicial power, because their ToS may impose[42] alternative dispute resolution systems to solve conflicts amongst users, based on the contractual provisions they define unilaterally.

37 See A. Narayanan, *Digital Feudalism Is Upon Us. How Do We Respond?*, Stanford Law School, 22 Jan. 2013, 2013; B. Schneier, *Power in the Age of the Feudal Internet*, in MIND, *Co:llaboratory discussion paper #6 Internet & Security*, 2013; L. Belli, *supra*, note 15, pp. 202-209; L. Belli and J. Venturini, *supra*, note 15, cit.

38 See R. MacKinnon, *Consent of the Networked: The worldwide struggle for Internet freedom*, Basic books, New York, 2012. 2012; L. Belli, *supra*, note 15.

39 See note 9.

40 See L. Belli – P. De Filippi, *Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation*, in European Journal of Law and Technology, Vol. 3, n°2, 2012; D. Korff, *The rule of law on the Internet and in the wider digital world*, Issue paper published by the Council of Europe Commissioner for Human Rights Council, 2014; L. Belli - J. Venturini, *supra*, note 15.

41 For a complete analysis of the decision giving rise to the so-called "right to be forgotten" and its consequences on Search engine capability to delist information, see H. Kranenborg, *Google and the Right to be Forgotten*, European Data Protection Law Review, 2015, 70.

42 In this regard, the aforementioned study by the Center for Technology and Society at FGV has demonstrated that 34% of the analysed contractual agreements imposed arbitration as the only method for dispute resolution. See <http://tinyurl.com/toshr>.

21 As pointed out by the OECD, even in the absence of legal compulsion, intermediaries frequently define and implement policies aimed at restricting the use of their systems in order to avoid liability for potentially illegal activities perpetrated thereon.[43] Moreover, many intermediaries establish so-called community guidelines, to define what content is admissible or inadmissible, and thereby avoid liability for user-generated content. In this context, the enforcement of the ToS and the community guidelines entail a wide spectrum of private policing activities, spanning from the implementation of algorithmic filtering to the active monitoring of users' publications by dedicated agents.[44] As mentioned above, such an approach has been encouraged by legislators to avoid the costs of rule-making, while letting intermediaries free to define efficient policies based on business best-practices.

22 Based on the distinction stressed in the previous section, we may argue that Internet intermediaries operate as special administrative police, with the goal of ensuring the order and morality within their systems, according to their own rules, while they act as judicial police to implement public law. The special police functions are performed in two diverse ways. First, when establishing the logical architecture of their systems, intermediaries create a self-performing police function within the very structure of their systems, which are configured to prohibit activities prescribed by the ToS and the legislation the intermediaries abide by. Second, intermediaries – and notably platform operators – may establish special teams dedicated to monitoring the activities of platform users to ensure compliance with the platform's own contractual regulation.[45] For example, Facebook can remove any content that is determined to violate its ToS thanks to hundreds of reviewers. Any user considered by Facebook as having posted such content is subject to the suspension or blocking of his or her account.[46] The same procedure is established by the majority of platforms, which explicitly foresee the possibility to terminate user accounts without previous notice and without allowing users to challenge the decision.[47] Furthermore, intermediaries act as judicial police, or at least judicial-police subsidiaries, by cooperating with law enforcement agencies, collecting evidence for enquires, and implementing court decisions through blocking, filtering and take-down measures.

23 As we will point out in the following section, the possibility of such cooperation – be it by virtue of a legal obligation or as a consequence of so called "voluntary commitments" – is turning intermediaries into an essential component of law enforcement mechanisms on a global scale.

C. Section II. The current EU trend on ISPs liability

24 In EU legal jargon, the term Internet Service Provider (ISP) generally refers to intermediaries that may play various roles as to the circulation of information online. In the beginning of the Internet era, most of the entities that qualified as ISPs did not deliver content protected by IPRs and were predominantly of a passive nature. However, to a limited extent they could facilitate the infringement of IPRs by their subscribers. Policy makers have therefore always been reluctant to excuse them from liability. The first generation of legislation introduced reflected this scepticism. Indeed, apart from residual circumstances,[48] the misconduct of intermediaries has generally been qualified as secondary or indirect liability. This was because ISP liability was incurred only when the primary infringer, who is a different subject from the ISP, has committed a direct violation.[49]

25 Recently, new and very active actors have gained prominence. These are actors that are providing platforms on which information can be created, edited and shared by users. They index and make such information searchable. They even create connections among different devices. Such an evolution constitutes a radical change of the general category of ISPs as well as the role of such players regarding the dissemination of information. A notable distinction has emerged between two types of providers. On the one hand, there are the service providers that are considered as "mere conduits of information",[50] and have an obligation to "treat all

43 See OECD, *supra,* note 16.

44 See note 4, 17 and 18.

45 *Idem*.

46 See *supra,* note 18. Facebook's ToS and policies can be found at <www.facebook.com/policies/?ref=pf>.

47 Such provisions can be found in 88% of the platforms analysed by the study on ToS and Human Rights, conducted by the Center for Technology and Society at FGV, which has also demonstrated that none of the analysed platforms commit to notifying users before proceeding with account termination. See *supra*, note 9.

48 For example, see Twentieth Century Fox Film Corp v. Newzbin Ltd [2010] EWHC 608 (Ch) (UK).

49 This can be also deduced from art. 8.3 of Directive 2001/29/EC, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:EN:PDF>, herein after the InfoSoc Directive; and from art. 11 of Directive 2004/48/EC, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:195:0016:0025:en:PDF>, herein after the enforcement directive.

50 See art 12, Directive 2000/31/EC, herein after "e-Commerce Directive", <http://tinyurl.com/ycs7q6jt>. Such provision is inspired by section 512 of the 1998 US DMCA, <https://www.copyright.gov/legislation/dmca.pdf>.

traffic equally".[51] On the other hand, there are the online service providers such as "online platforms".[52] The latter group undertakes a more active role in the organisation and circulation of information. As a result, policy makers have recently re-focussed their attention on intermediaries. The attention is particularly focussed on aspects of potential liability when the intermediary is deemed as an active ISP.

26 Considering the impact liability-related rules can have on the online environment, a predictable and clear perimeter of intermediary liability is essential to ensure overall legal certainty and to enable access to effective remedies in case of an infringement. Notably, secondary liability of intermediaries is considered the only efficient strategy to compensate right holders in the event their IPRs are infringed, and the infringers are difficult to catch. It is crucial to understand however, that in the event intermediaries are considered as strictly liable, this would unreasonably and negatively affect legitimate information dissemination. This may in turn jeopardise the free flow of information and innovation. Consequently, ISP liability rules should be clearly designed, with particular regard to limitations and the so-called "safe harbours" for intermediaries. The clear establishment of "safe harbours" is indeed essential to balance the different, but equally important interests involved in the digital realm. These include the users' interest to have the greatest possible access to information and innovation. Similar interests that warrant protection include the potentially competing interest of any subjects producing and those disseminating content for business purposes or any other purpose.

27 The scope of the "safe-harbours" has been a subject of discussion in recent years. In the EU, the overall goal of fostering market growth has been used as a justification for renewing attention on the topic, for over twenty years.[53] The issue in the current debate is thus the same as the one preceding the introduction of the (still) current general legal framework on ISP liability within the e-commerce Directive. It refers to how to (re-)design ISP's liability to foster market growth. The technical and social framework is very different from the one in which the e-commerce Directive was discussed, particularly because platforms are now deep-rooted elements of the Internet ecosystem and are considered to be covered by the notion of the ISP. What differs in today's discussions is the approach used and suggested by decision-makers. In fact, the rationale of the existing framework is that the sound protection of rights shall be ensured to boost market growth. Such an approach can be found in the data protection rules,[54] in some decisions of the European Court of Justice (EUCJ) and the European Court of Human Rights (ECHR).[55] Furthermore, the EU legislator decided to align with this trend, introducing ISP-liability-related principles in the proposal for a new copyright directive.[56] Considering the preparatory works of the upcoming reform,[57] it is not excluded that the revision of the current enforcement Directive 2004/48/EC will follow the same trend.

28 For the time being, the e-commerce Directive remains untouched, although the complexity of the current technical and social context brings about more challenges compared to previously. A sectorial approach may appear as the most effective to face these challenges, although it may not be ideal to face such complexity. However, as we discuss in Section III and in the Conclusion, the consistency of the current sectorial approach with the *acquis communautaire* remains unclear and the method currently used, risks leading to further contradictions in the overall

51 See art 3, Regulation 2015/2120/EU of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access, <http://tinyurl.com/ycwjxcz2>.

52 See Opinion of the Committee on Legal Affairs for the Committee on Industry, Research and Energy and the Committee on the *Internal Market and Consumer Protection on online platforms and the Digital Single Market* (2016/2276 (INI)), <http://tinyurl.com/ybxl33pw>.

53 See *e.g.* M. Horten, *A Copyright Masquerade: How Corporate Lobbying Threatens Online Freedoms*, Zed Books, 2013.

54 See directive 95/46/EC, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>, herein after Data Protection Directive, containing among others references to controllers. It has to be reminded that search engines qualify as data controllers under the Guidelines on the Implementation of the EUCJ case Google Spain v. Costeja, 14/EN WP 225 of 26 November 2014, available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf>. For an analysis on the ISPs liability, focusing on the interferences between the e-commerce Directive and the directive on data protection see B. Van der Sloot, *Welcome to the Jungle: the Liability of Intermediaries for Privacy Violations in Europe*, *JIPITEC* 2015, 3, p. 215ff. Additionally, see the Data Protection Regulation 2016/679, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC>, which reminds us that all the principles embedded in the text are without prejudice to the application of the e-commerce Directive, in particular arts. 12 – 15, and at the same time introduces among others the right to data portability and the right to resist profiling, plus several obligations for controllers, which may affect active ISPs.

55 The case law of the EUCJ and of the ECHR is mentioned and sum up by the project *The World Intermediaty Liability Map*, Center for Internet and Society at Stanford, <http://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap>.

56 See Proposal for a Directive of the European Parliament and of the Council of 14 September 2016 on Copyright in the Digital Single Market, <https://ec.europa.eu/digital-single-market/en/news/proposal-directive-european-parliament-and-council-copyright-digital-single-market>, herein after the proposal directive on Copyright.

57 See *infra*, note 94.

legal framework,[58] thereby reducing legal certainty and harmonisation, rather than increasing it. Furthermore, such an approach risks negatively affecting the users' freedom of expression, as well as the freedom of ISPs to conduct a business. In the latter case, it unduly limits the chances to enter and remain competitive in the market, particularly for platforms. Consequently, we argue that it seems over-optimistic to think the proposed strategy will favour the achievement of a (Digital) Single Market. On the contrary, such an approach may foster a less eclectic market, where questions as to the fundamental freedom to conduct a business,[59] and the freedom of expression arise, while antitrust-related issues will remain unsolved.

I. How did we get here?

29 The international legal framework on copyright or related rights does not embed express rules on the liability of ISPs. The 1996 WIPO Copyright Treaty (WCT) only concerns the right of communication to the public of the right holders. Nevertheless, in the Agreed Statements Concerning the WCT, article 8 states: "... it is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty [...]"[60] Such a provision is considered to indirectly provide "safe harbours" for technological intermediaries.

30 In the same period as when the WCT was negotiated, national policymakers started developing rules on ISP liability. Policy makers introduced exceptions and the so-called "safe harbours".[61] Notably, the European debate of the late nineties focused on ISP liability, but from a market growth perspective. Such discussions led to the introduction of the e-commerce Directive that, amongst its main purposes, aimed at limiting legal uncertainty by harmonising the different national approaches to ISP liability for wrongful conduct carried out by their users through their systems. According to the e-Commerce Directive, no general obligation to monitor the stored or transmitted information was imposed on the ISPs, nor a general obligation to actively seek facts or circumstances indicating illegal activity.[62] Indeed, such an obligation would have been considered a disproportionate burden for any ISP and a barrier to economic development. In addition, the e-commerce Directive introduced horizontal,[63] "safe harbours", relieving ISPs from liability in three different cases. Firstly, art. 12 of the e-commerce Directive excluded liability for mere conduits, by specifying that access providers are not liable for the information transmitted on the condition that they: (a) do not initiate the transmission; (b) do not select the receiver of the transmission; and (c) do not select or modify the information contained in the transmission. Hence, when they remain passive, providers may have very limited additional responsibilities. Secondly, art. 13 of the e-Commerce Directive was about caching, which never raised relevant concerns. Thirdly, art. 14 stated that a hosting provider is not liable for the information stored, as long as: (a) the provider does not have actual knowledge of the illegal nature of the 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; and (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.[64]

31 This legal framework has often been criticised for being obsolete since its introduction. Considering the high speed at which technology evolves, contrasted against the much lower speed of the policy and legal debate, this is no surprise. The first direction taken by national and EU judges, and subsequently by legislators, undoubtedly led to further strengthening the ISPs' duty to care and more broadly speaking, the ISPs' liability. This is not surprising either.[65] This is aligned to the overall

58 B. Van der Sloot, *supra* note 54, 215ff. Critics to the shifting from a horizontal to a sectorial/vertical approach are also expressed by G. Frosio, *Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy*, *Northwestern University LR Online* 2017, forthcoming.

59 See supra, note 6. For an analysis of this fundamental freedom (related to ISPs) appearing only in this Charter (and in some national constitutions) see C. Geiger – E. Izyumenko, *The Role of Human Rights in Copyright Enforcement Online: Elaborating a Legal Framework for Website Blocking*, *American International University Law Review* 2016, p. 43ff.

60 See <http://www.wipo.int/treaties/en/text.jsp?file_id=295456>.

61 The earliest country to enact new copyright statutes to comply with international framework and deal with digital challenges was the USA. For some remarks on the US legal framework J. Ginsburg – R. Gorman, *Copyright Law (Concepts and Insight Series)*, Foundation Press, p. 219ff.; see also X. Amadei, *Standards of Liability for Internet Service Providers: A Comparative Study of France and the US with a Specific Focus on Copyright, Defamation and Illicit Content*, *Cornell Int'l L.J.* 2001-2002, p. 189ff. As to the solutions adopted in other jurisdictions see the project *The World Intermediary Liability Map*, cit.

62 Art. 15.

63 P. Van Eecke, *Online Service Providers and Liability: A Plea for a Balanced Approach*, *Common Market LR* 2011, p. 1455ff., notes that when ISPs mentioned in the e-commerce Directive meet the requirements of its section IV, they will be exempted from contractual, tortious, criminal, administrative, or any other type of liability, "for all types of activities initiated by third parties, including trademark infringement, defamation", etc.

64 The outcome of the e-commerce Directive is quite close to the one of the DMCA and subsequent section 512 of the Copyright Act.

65 The possibility for strengthening the regime has been in the

approach EU policy-makers have had for years to the protect IPRs. In other words, the approach used implies that the more technological facilities are able to enhance the circulation of information, the stricter the legal rules would be. Consequently, chances to enhance the circulation of information have reduced. Such an approach is led by the belief that protectionism would favour market growth. Indeed, the EU legislator has been trying to close the "value gap". This value is derived from revenues generated as a result of the online exploitation of copyrighted material. Allegedly, the revenues are unfairly distributed between the different players of the online-publishing value chain.[66] The surprising element is the lack of evidence as to the fact that a (very) protectionist environment fosters creativity and development.[67] However, neither policymaking efforts nor jurisprudence seems to have taken this lack of evidence into account.

II. Some jurisprudential clarifications of the intermediary liability regime

32 The introduction of the e-Commerce Directive was supposed to provide legal certainty to ISPs that desperately needed to know when they may be considered as (indirectly) liable, and what measures to take to avoid any liability.

1. From indirect to direct liability

33 The EUCJ focused on the notion of communication to the public while ruling on several cases related to the interface between the e-commerce Directive and the Copyright directive. In particular, the Court of Luxembourg qualified re-transmission of a terrestrial television broadcast over the Internet,[68] linking,[69] and framing,[70] as a communication to the public. In other words, it was a copyright owner prerogative. From this jurisprudence, it is possible to draw at least two conclusions. First, the overall trend is to confirm the broad scope of the copyright holder's economic right of communication to the public. The details of this trend are however sometimes confusing.[71] This may suggest that the EUCJ is trying to find the best way to solve complex problems. As foreseen by art. 21 of the e-commerce Directive, for the best way to find an appropriate and reasonable solution, it has now become necessary to assess the economic, social and legal impact of linking. Second, these decisions are confirming ISPs may be liable for secondary or indirect liability, depending on the presence of an infringement to the right of the communication to the public.[72] However, the very recent Pirate Bay (Ziggo) case, seems to have introduced direct liability for the ISP.[73] The reason of this major change might be found in the Opinion of the Advocate General, who argued that the problem of online infringement needs a harmonised EU answer.[74]

34 It is likely that primary liability has the effect of pushing ISPs to enhance any activity and implement

EU legal framework since the beginning: see for instance Recital 48 of the e-commerce Directive.

66 The notion of value gap was introduced by the music industry and endorsed by the EU legislator in the draft proposal directive on copyright. It has to be added that a distinction is usually drawn in this regard between subscription-funded platforms (Spotify, Netflix) requiring the consent of right holders to operate legally, and ad-funded platforms (YouTube, Dailymotion), growing thanks to user-generated content. As a result, they tend to focus on notice-and-take-down systems and not on licensing.

67 G. Frosio, *Digital Piracy Debunked: A Short Note on Digital Threats and Intermediary Liability*, *Internet Policy Review* 2016, p. 1ff., where the author explains that the literature has demonstrated to a certain degree of consistency that there is an added value to promote, rather than a value gap to close.

68 EUCJ, 7 March 2013, C-607/2011, case *TVCatchup*, *EIPR* 2016, p. 580ff. In the same sense EUCJ, 26 March 2015, C-279/13, case *Sandberg*, <www.curia.eu>.

69 See EUCJ, 13 February 2014, C-466/12, case *Svensson*, commented by C. Koonen, *The Use of Hyperlink in an Online Environment: Putting Links in Chain*, *Grur int*. 2016, p. 867ff. The Court ruled that linking infringes the copyright holders' exclusive rights only when it reaches a "new public". This latter is a not supported notion by international and regional copyright legal tools, according to P. Mezei, *Enter the Matrix: the Effects of the CJEU Case Law on Linking and Streaming Technologies*, *Grur Int*. 2016, p. 887ff., spec. 900. See also EUCJ, 8 September 2016, C-160/15, case *GS Media*, <www.curia.eu>, stating that a link to materials for which the copyright holder didn't authorise the uploading/availability to the public was infringing communication to the public when he had sufficient knowledge of the unauthorized upload of the linked work.

70 EUCJ, 21 October 2014, C-348/13, case *BestWater*, <www.curia.eu>, issuing a reasoned order under art. 99 of the Rule of Procedure of the EUCJ, and applying the findings of the *Svensson* decision to the "framing".

71 For an analysis of the EUCJ case law on the right of communication to the public assessing that in its interpretation of Directive 2001/29 (Article 3) and Directive 2006/115 (Article 8), the Court deviated from not only the meaning which is generally conferred upon these provisions, but also from internationally-recognized solutions see P. Sirinelli – JA. Benazeraf – A. Bensamoun, *CSPLA, Mission: Droit de Communication au public*, Final Report of December 2016, <http://www.culturecommunication.gouv.fr/Thematiques/Propriete-litteraire-et-artistique/Conseil-superieur-de-la-propriete-litteraire-et-artistique/Travaux/Missions/Mission-du-CSPLA-sur-le-droit-de-communication-au-public>, spec. Section 2, Appendix 5 and 6.

72 See E. Rosati, *Why a Reform of Hosting Providers' Safe Harbour Would be Unnecessary Under EU Copyright Law*, *EIPR* 2016, p. 668ff.

73 EUCJ, 14 June 2017, C-610/15, case *Pirate Bay*, available on the official website of the EUCJ, <www.curia.eu>.

74 Opinion of Advocate General Szpunar, 8 February 2017, C-610/10, *Stichtin Brein v. Ziggo Bv*, available on the official website of the EUCJ, <www.curia.eu>.

any measure that may reduce the risk of incurring liability. The implementation of (even) more voluntary and technological filtering measures, as well as notice-and-take-down systems, are to be expected. This is in turn strengthening the ISPs' private-regulation-and-police capabilities.

2. Some remarks on the scope of injunctive intervention

35 National (lower) courts were called to issue a decision on the scope of injunctive intervention. The decisions included the take-down of notified infringing material, as well as proactive monitoring, with the aim of preventing future infringements.[75] The courts often used the margin of appreciation they had. Consequently, as case law may reveal, the initial decisions were confusing.[76]

36 When the EUCJ was asked to interpret the relevant copyright enforcement and e-commerce Directive rules on preventive filtering measures, it ruled that injunctions requesting preventive filtering systems addressing all the customers of an ISP were to be precluded.[77] The argument used to reject such systems was the incompatibility of the implementation of preventing filtering with the principle of proportionality as well as with the lack of a general obligation to monitor.[78] This case law was clearly aimed at safeguarding two interests. On the one hand, it safeguarded the interest of the ISPs as market operators, for whom such overarching filtering systems would have endangered "the freedom to conduct business enjoyed by operators such as ISPs." This is deemed to also include the right for any business to be able to freely use - within the limits of its liability for its own acts - the economic, technical and financial resources available to it. On the other hand, the Court reinforced the interests of users. The court argued that the propped filtering systems could have infringed "the right of costumers to protect their personal data and their freedom to receive or impart information."[79] Such decisions have therefore clarified that a general obligation to monitor is to be considered disproportionate.

37 Besides, the EUCJ ruled in favour of court injunctions that do not specify what measures an Internet Access Provider (IAP) must take to block access to websites making available copyrighted material without the right holder's permission. The Court stated that blocking orders may be imposed on access providers when they can avoid penalties by showing that they have taken all reasonable measures. The Court affirmed that national courts are entitled to issue blocking orders against IAPs, arguing that fundamental rights in the EU do not preclude court injunctions prohibiting an ISP from "allowing its customers access to a website placing protected subject-matter online without the agreement of the right holders".[80] However, these injunctions must be balanced with the public interest to access the information, for only reasonable injunctive measures may be accepted. This case also created the opportunity to debate the proportionality of an injunctive measure, in particular if that injunctive measure is related to the fundamental interests of the ISPs. This interest includes the freedom to conduct a business. Indeed, the adoption of an injunction limits such freedom, because it may:

> *... [C]onstrain its addressee in a manner which restricts the free use of the resources at his disposal because it obliges him to take measures which may represent a significant cost for him, have a considerable impact on the organization of his activities or require difficult and complex technical solutions.*[81]

38 However, an injunctive measure does not seem to infringe the very substance of the freedom of an ISP to conduct a business because it "leaves its addressee to determine the specific measures to be taken in order to achieve the result sought, with the result that he can choose to put in place measures which are best adapted to the resources and abilities available to him."[82]

39 In other words, the EUCJ cannot preclude injunctions, namely because they are enabled by Recital 45 of the e-commerce Directive, art. 8.3 of the InfoSoc Directive,[83] and by art. 11 of the enforcement

75 For a comparative and detailed perspective see C. Angelopolous, *Beyond the Safe Harbors: Harmonizing Substantive Intermediary Liability for Copyright Infringment in Europe*, 2016, <https://www.ivir.nl/publicaties/download/1087>.

76 See cases recorded in the *World Intermediaty Liability Map*, cit.

77 EUCJ, 24 November 2011, *supra* note 5. In the same sense EUCJ, 16 February 2012, C-360/10, case *SABAM v. Netlog NV*, *EIPR* 2012, p. 791ff. commented by S. Kulk - F. Borgesius, *Filtering for copyright enforcement in Europe after the Sabam cases*. In addition, EUCJ, 12 July 2011, C-324/09, case *L'Oréal*, available on www.curia.eu.

78 This principle was clearly emphasised by EUCJ, C-70/10, case *Scarlet*, cit.; and EUCJ, C360/10, case *SABAM v Netlog NV*, cit., § 53.

79 The freedom of (imparting) information can be also considered an interest of ISPs.

80 EUCJ, C-314/12, case *Telekabel*, cit.

81 *Idem.*

82 *Ibid.*, §§ 48 – 53. In particular, the Court specified that the exoneration applying when reasonable measures are taken seems justified in light of the fact that he is not the author of the infringement of a fundamental IPR that has led to the adoption of the injunction. One could wonder whether the more recent case law and in particular the *Ziggo* case does not change this approach.

83 On the German choice to not implement art. 8.3, but relying on courts to implement the principle embedded into the

Directive,[84] which establish such provisions. However, it precludes them when they are not aligned with other fundamental principles, such as proportionality, and when they affect constitutional freedoms, such as the freedom to conduct a business or freedom of information.[85]

40 It is important to note that several issues and potential concerns are intertwined with the injunctions,[86] by which operators are ordered to block the perpetrator of IPR infringement to prevent any repetition of infringements, or to take measures that allow easy identification of the perpetrator. First, a blocking technique may lead to over-blocking. Over-blocking is when legitimate content is unduly blocked.[87] These techniques may still be circumvented quite easily.[88] Secondly, the implementation of this remedy to IPR infringement may be particularly cumbersome, because multiple proceedings need to be filed, thereby raising the complexity and the related-cost of the remedy. Notably, the cost remains one of the main impediments, if not the main one. Since the economic burden of any kind of blocking injunction will be sustained by the intermediary,[89] one may question both the proportionality of such a burden and its interference on the intermediary's freedom to conduct a business. These may be some of the reasons why an extra-judicial remedy - such as the notice-and-take-down procedure - was developed and now appears to be favoured by the EU legislator.

D. Section III. The Undergoing (R)Evolution

41 *De iure condendo*, the EU legislator has recently taken several initiatives that further erode "safe harbours". Conspicuously, several communications of the European Commission are suggesting and anticipating the upcoming legislative steps of the EU legislator. For instance, the EC proposes to introduce filtering obligations and voluntary measures.[90] It anticipates that legislative action will be taken in respect of linking, news aggregators, as well as some enforcement-related aspects as notice and action mechanisms. This is in terms of the take down and stay down principle.[91] In particular, it seems to endorse the idea that the e-commerce Directive will remain untouched.[92] However, specific issues such as cyber-bullying, terrorism, incitement through hatred, harmful content addressing minors in particular, and IPR infringements, will be prevented by sectorial initiatives. This will be done by amending

InfoSoc Directive, see C. Angelopolous, (2016), cit., p. 12ff.; M. Schaefer, *ISP Liability for Blocking Access to Third Party Infringing Content*, *EIPR* 2016, p. 633ff.

84 See EUCJ, C-324/09, case *L'Oréal*, cit., where the Court interpreted Article 11 of the Enforcement Directive as meaning that an ISP may be ordered "to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of that kind".

85 For an analysis see Geiger – L. Lu, *The Evaluation and Modernisation of the Legal Framework for the Enforcement of Intellectual Property Rights*, Research Paper No. 2015-03, Centre for International Intellectual Property Studies (CEIPI), 11 May 2016, <https://ssrn.com/abstract=2966839> or <http://dx.doi.org/10.2139/ssrn.2966839>.

86 At the national level, the Netherlands has for a long time been one of the few countries which tried, but has not succeeded (yet) to obtain a blocking injunction for an ISP: see K. van den Heuvel, *Next Chapter on ISPs Blocking Battle: Dutch Supreme Court Refers Questions About Indirect Infringement by Operators of the Pirate Bay to the CJEU*, *EIPR* 2016, 577ff. For an analysis of the cases in France, Germany and UK see C. Angelopolous, (2016), cit., p. 12ff.

87 See *supra* note 3.

88 Roy – A. Marsoof, *Blocking Injunctions and Collateral Damage*, *EIPR* 2017, p. 74ff., which is suggesting that the only option with no related collateral damage is the blocking of URL (very easy to be circumvented, though). See also, Roy – A. Marsoof, *The Blocking Injunction: A Comparative and Critical Review of the EU, Singaporean and Australian Regimes*, *EIPR* 2016, p. 9ff., where the authors explained the UK judicial innovation according to which once an injunction is filed, the right holders can notify ISPs directly when an online location changes its IP address or URL without applying to court. This enables right holders to monitor online changes and ask ISPs to update their blocking databases, thus eliminating the impact of any circumvention.

89 K. Frolova-Fox – J. Jones, *Getting the Look for Less: the Blocking Cost: Cartier Internaitonal v. BSkyB (Court of Appeal)*, *EIPR* 2017, p. 58ff.

90 EC, *Communication: A Digital Single Market Strategy For Europe*, COM(2015), 6 May 2015, <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX%3A52015DC0192>. In addition, a proposal of the Audio-Visual Media Services Directive was issued on 25 May 2016 and it is now available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1464618463840&uri=COM:2016:287:FIN>. Such a proposal imposes platforms to put in place ("preferably through co-regulation", says the proposal) measures protecting from incitement to hatred and particularly minors from harmful content. This may be in conflict with the absence of a general obligation to monitor ISPs as imposed by the e-commerce Directive.

91 EC, *Communication: Towards a Modern, More European Copyright Framework*, COM(2015), 9 December 2015, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A626%3AFIN>.

92 EC, *Communication: Online Platforms and the Digital Single Market Opportunities and Challenges for Europe*, 25 May 2016, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0288&from=EN>. This communication was based upon a public Consultation that the EC launched, of which outcome is in the *Full Report on the Regulatory Environment for Platforms, Online Intermediaries and the Collaborative Economy*, <https://ec.europa.eu/digital-single-market/en/news/full-report-results-public-consultation-regulatory-environment-platforms-online-intermediaries>. The consultation mentioned (but the communication does not) additional categories of ISPs to be implemented besides caching, conduit, hosting and that may enjoy the exemption; the consultation discussed new business models and services, such as cloud service providers, linking services and search engines.

Copyright rules and Audio-Visual related rules,[93] but not limited thereto. As an overall result, the strategy seems to turn ISPs into cyber-regulators and cyber-police. All this, without intervening on the e-commerce Directive directly.[94]

42 As an upcoming legislative step, the Proposal Directive on copyright has been criticised for several reasons. One such reason is based on the two main clauses affecting the liability of ISPs.[95] The first critique refers to the introduction of a neighbouring right for the digital press. This affects the ISPs' liability regime. It is likely that it obstructs innovation rather than fostering it. The second reason focusses on art. 13 and the related Recitals 37, 38, and 39 of the proposal on the liability of ISPs. These clauses would apply to active hosting providers that store and provide access to protected works and cannot benefit art. 14 of the e-commerce Directive. The exemption does not apply to active host providers. These are those ISPs that go beyond the mere provisions of physical facilities.[96] These ISPs would need to conclude licensing agreements with right holders. The text does not clarify whether a not-completely-passive host provider, which is unable to control the data stored, can benefit from the safe harbour, as Recital 42 of the e-commerce Directive suggests.[97] Furthermore, Recital 38 refers to the communication to the public, as an act performed by an ISP. The doctrine interpreted this wording as the reference to a primary liability[98] for ISPs, for infringements materially committed by others. Unless this recital merely contains unfortunate wording, which would not imply any shift from indirect to direct liability, and which seems to be excluded,[99] this would be aligned with the recent Ziggo case.

43 A very problematic point of these recitals and article is their encouragement to deploy a monitoring system, such as content-recognition technologies to prevent the availability of infringing content. This approach is evidently in conflict with art. 15 of the e-commerce Directive, which forbids any general monitoring obligations. Furthermore, it goes against art. 3 of the Enforcement Directive and is not aligned with the EUCJ case law, which particularly recognised the need for "fair balance" between the various fundamental rights at stake, such as the freedom to conduct a business (endangered by the disproportionate burdens on ISPs), the protection of personal data, and the freedom of expression (endangered by a massive control by ISPs). Nevertheless, it should be specified that the e-commerce Directive and the EUCJ merely ban measures aimed at general monitoring, while only filtering systems applying to specific cases could be

93 As a result, the EC recently promoted a step towards the privatization of law enforcement online through algorithmic tools implemented by major providers. See note 15.

94 It has to be added that in parallel to the aforementioned initiatives, the EC launched a public consultation to seek feedback from stakeholders (right holders, judges and law practitioners, intermediaries, public sector bodies, consumers) as to their satisfaction with the enforcement framework. See EC, *Consultation on Evaluation and Modernization of the Legal Framework for the Enforcement of IPRs*, 9 December 2015, of which results are in the related *Summary of responses*, <http://ec.europa.eu/growth/industry/intellectual-property/enforcement_en>. For a comment see X. Seuba – C. Geiger – L. Lu, (2016), cit. At the same time, was launched EC, *Consultation on Due Diligence and Supply Chain Integrity*, 9 December 2015, of which results are in the related *Report*, <http://ec.europa.eu/growth/industry/intellectual-property/enforcement_en>, aimed at gathering information, in particular from SMEs, to allow the mapping and promotion of best practices protecting supply chains from IPRs infringement threats. These consultations were launched because the Communication on the *Digital Single Market Strategy for Europe* announced that the EC would have made a proposal to modernise the enforcement measures in IPRs, focusing on commercial-scale infringement as well as cross-border applicability. The proposal was expected by 2016, while nothing has been released yet. However, it is not unlikely that special injunctions against online ISPs will be introduced. Hopefully, some clearer information will be provided as to the criteria for defining the proportionality of an injunction; and the new Directive will clarify the EUCJ case law on how to balance the effective implementation of an injunctive measure and the right to freedom of information of users in case of a blocking order that does not specify the measures which a service provider must take. Finally, EC, Communication on *Promoting a fair, efficient and competitive European copyright-based economy in the Digital Single Market*, 14 September 2016, <https://ec.europa.eu/digital-single-market/en/news/promoting-fair-efficient-and-competitive-european-copyright-based-economy-digital-single-market>, was released, which evokes the injunctive measures against ISPs.

95 Among the reasons justifying critics, there is inconsistency in the wording of the preparatory works (Explanatory Memorandum, the Impact Assessment), the Recital and the text of the proposal, identified by C. Angelopolous, *On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market*, 2017, <https://ssrn.com/abstract=2947800>. The different terms used for referring the same obligations are complicating the task to the interpreters.

96 It is thus necessary to verify whether an ISP plays an active role on a case-by-case basis. This principle is clearly inspired by EUCJ, C-324/09, case *L'Oréal*, *cit*.

97 As well as the *L'Oréal* case does. The fact that the wording of this part of art. 13 has been inspired by this *L'Oréal* case could be used as an argument to support this thesis. However, C. Angelopolous, (2017), cit., does not seem convinced about the fact that the clause is consistent with art. 14 of the e-commerce Directive.

98 A. Lehman, *Intellectual Property and the National Information Infrastructure: the Report of the Working Group on Intellectual Property Rights*, DIANE Publishing, 1995, p. 114ff., underlines that back in the nineties, the safe harbours were eventually introduced in the US, while the first proposal was to introduce primary liability for ISPs for any infringement.

99 In this sense see C. Angelopolous, (2017), cit.; G. Frosio, *From Horizontal to Vertical: an Intermediary Liability Earthquake in Europe*, Oxford Journal of Intellectual Property and Practice 2017, forthcoming.

allowed.[100] However, practically speaking, it is hard to understand how such a system could work.[101]

44 The proposal indicates that platforms should take voluntary measures to curtail infringing activities. However, the inconvenience that voluntary measures bring along are quite clear. First, they can be the source of a disharmonised patchwork of practices, which goes against the wish to create a single market. Moreover, they introduce privately-enforced standards, based on the cost reduction and private interest maximisation rather than legal obligations enforced by the judiciary authorities. Indeed, proactive monitoring, as well as notice-and-take or stay-down regimes, are a clear step in the direction of privatisation of online enforcement.[102] It still has to be proven that this kind of private enforcement may be considered, and under which circumstances, yet remain fully respectful of the numerous fundamental rights involved. In the meantime, scepticism is permissible.

E. Conclusion

45 Internet intermediaries are essential gateways for users to seek, disseminate and receive information and ideas, enabling users to learn and become innovators in their own right. Users play an instrumental role in the circulation of knowledge and innovation. In addition, due to their position as chokepoints, intermediaries become key allies of law enforcement agencies and prosecutors, to implement national legislation. It is necessary to caution against excessive involvement by and a "responsibilisation of intermediaries", which may effectively delegate *de facto* regulatory and police functions to private entities. Intermediaries have now become increasingly active, in particular, but not only, by fostering user-generated content, by indexing information, and making it searchable. Simultaneously, several ISPs have begun taking voluntary commitments to curb and discourage illicit activities and the access to unlawful content by their users. In principle, all ISPs can benefit from "safe harbours", shielding them from liability, as foreseen by the e-commerce Directive. However, the European Court of Justice and the EU written rules *de iure condendo* seem to request an extraordinary duty of care when an ISP is an active ISP. In other words, the more active ISPs are, the higher duty of care is imposed on it. Consequently, the ISP will be encouraged to adopt more private regulation and private policing.[103] This situation is raising scepticism regarding respecting fundamental rights and freedoms of the end user, such as the freedom of expression and the right to privacy. Furthermore, the intermediaries' freedom to conduct a business can also be seriously endangered by this increasingly stricter approach, while, as we have emphasised, the consistency of the current sectorial approach with the *acquis communautaire* remains unclear and may reduce legal certainty, rather than increasing it.

46 In light of the role played by ISPs and the significant impact their private ordering can have on Internet users' rights, such entities are expected to behave in accordance with their responsibilities to respect human rights. Notably, while international law does not consider private actors as having a positive obligation to protect human rights, as public actors do, it is important to stress that every business actor has a responsibility to respect human rights, as affirmed by the UN Guiding Principles on Business and Human Rights.[104] From this perspective, the intermediaries' "responsibilisation" would impose a prohibition to refrain from the violation of users' human rights and to provide effective remedies to repair any negative consequences of their private ordering on their users.[105] However, the concept of the IPS' "responsibilisation" does not seem to be prevalent. The recent tendency towards "responsibilisation of Intermediaries" seems to go in the opposite direction; not only by stimulating voluntary commitments, but also by imposing legal obligations to police cyberspaces. This is exemplified by the recent German law on Enforcement on Social

100 See Recital 47 and art. 14.3, e-commerce Directive. On the notion of "specific case" see P. Van Ecke, *Online Service Providers and Liability: A Plea for a Balanced Approach*, *Common Market Law Review* 2011, p. 1455ff., spec. 1457ff., explaining that the monitoring obligation shall be considered as an exception and therefore interpreted narrowly, the scope and the amount of the expected to be identified infringements have to be narrow as well, the material constituting an infringement must be obvious.

101 Will there be notices? Counter-notices? Is a filtering system consistent with notices and (if any, also subsequent) counter-notices? See the doubts shared by G. Frosio, *supra* note 58.

102 This general trend would push to favour a shift from liability to responsibility of ISPs that would police with self-intervention and algorithmic enforcement allegedly infringing activities over the Internet. See G. Frosio, *supra* note 58. Not to mention that any new market entrant should actually license filtering technology from big platforms such as Google/YouTube, which may keep it for their exclusive use. As most of the platforms/market players are US-based, this evolution may create a EU market controlled by US-based businesses.

103 B. Van der Sloot, *supra* note 54, p, 222.

104 See report of the Special Representative of the Secretary - General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie: *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, UN Human Rights Council Document A/HRC/17/31, 21 March 2011.

105 In this sense, see the work of the UN IGF Dynamic Coalition on Platform Responsibility, notably L. Belli, P. De Filippi, N. Zingales (eds.), *Recommendations on terms of service & human rights*, Outcome Document n°1, 2015, <tinyurl.com/toshr2015>.

Networks.[106] It should be noted that, although the delegation of regulatory and police functions to ISPs may seem efficient to avoid inconclusive political debates, self-regulatory measures may be counterproductive, reduce harmonisation, and result in being clearly less satisfactory than the adoption of a comprehensive framework. Hence, from a practical perspective, the sectorial approach and the encouragement of voluntary measures run the very serious risk of creating a lack of consistency with the current and upcoming norms that relate to the issue at hand.

47 As suggested by the empirical evidence, although a move towards privatisation of online enforcement via extra-judicial measures seems to be a worldwide trend, this is not necessarily the "fairest balance" needed between the fundamental competing interests. First, measures such as notice-and-take-down and filtering can negatively affect user privacy,[107] stifle the dissemination of information, while imposing a disproportionate economic burden on the ISPs. In this sense, ISPs are increasingly pleading for freedom of information to limit the supply of data about users (suspected to have carried out unlawful activities via their networks), to third party right holders, or to avoid monitoring their networks to detect or block illegal activities and content. This situation potentially harms privacy and freedom of expression, but also the freedom to conduct a business. This freedom may be severely limited as a result of a disproportionate burden of formalities imposed on intermediaries. Consequently, fewer and fewer intermediaries may be able to enter or remain in the market. This may negatively affect competition. Second, should the "safe harbours" be re-designed to ensure a healthier balance between the protection of content creators, right holders and users' interests, this should be carried out based on empirical evidence. There is currently no evidence that "closing the value gap" by adding more protection to economic rights or designing stronger rights would favour creativity and cultural production. On the contrary, there is factual evidence that more flexibility and less stringent IPR protection can foster creativity.[108]

106 See *supra* note 20.

107 On privacy-related aspects see J. Jie Hua, *Establishing Certainty of Internet Service Provider Liability and Safe Harbor Regulation*, *National Taiwan University Law Review* 2014, <https://ssrn.com/abstract=2591222>; and B. Van der Sloot, *supra* note 55.

108 G. Frosio, *supra,* note 67.

The Death of 'No Monitoring Obligations'

A Story of Untameable Monsters

by **Giancarlo F. Frosio***

Abstract: In imposing a strict liability regime for alleged copyright infringement occurring on YouTube, Justice Salomão of the Brazilian Superior Tribunal de Justiça stated that "if Google created an 'untameable monster,' it should be the only one charged with any disastrous consequences generated by the lack of control of the users of its websites." In order to tame the monster, the Brazilian Superior Court had to impose monitoring obligations on Youtube; this was not an isolated case. Proactive monitoring and filtering found their way into the legal system as a privileged enforcement strategy through legislation, judicial decisions, and private ordering. In multiple jurisdictions, recent case law has imposed proactive monitoring obligations on intermediaries across the entire spectrum of intermediary liability subject matters. Legislative proposals have followed suit. As part of its Digital Single Market Strategy, the European Commission, would like to introduce filtering obligations for intermediaries in both copyright and AVMS legislations. Meanwhile, online platforms have already set up miscellaneous filtering schemes on a voluntary basis. In this paper, I suggest that we are witnessing the death of "no monitoring obligations," a well-marked trend in intermediary liability policy that can be contextualized within the emergence of a broader move towards private enforcement online and intermediaries' self-intervention. In addition, filtering and monitoring will be dealt almost exclusively through automatic infringement assessment systems. Due process and fundamental guarantees get mauled by algorithmic enforcement, which might finally slay "no monitoring obligations" and fundamental rights online, together with the untameable monster.

Keywords: Proactive monitoring obligations; filtering obligations; intermediaries; fundamental rights online

Recommended citation: Giancarlo F. Frosio, The Death of 'No Monitoring Obligations': A Story of Untameable Monsters, 8 (2017) JIPITEC 199 para 1.

A. Introduction

1 In the next few pages, I will be telling you a story that is in between a dark fairy tale and mystery fiction. This story is filled with monsters—untamable ones—and its protagonist has been murdered or at least might be in danger of sudden death. However, let us start from the beginning as any good story is supposed to start.

2 Once upon a time there was "no monitoring obligation." Traditionally, online service providers have enjoyed an exemption to any general obligation to monitor the information, which they transmit or store or actively seek facts or circumstances indicating illegal activity.[1] Together with safe harbor provisions that impose liability on hosting providers according to knowledge-and-take-down,[2] the "no

* Senior Researcher and Lecturer, Center for International Intellectual Property Studies (CEIPI), Universitè de Strasbourg; Non-Resident Fellow, Stanford Law School, Center for Internet and Society. The author can be reached at gcfrosio@ceipi.edu.

1 See eg Council Directive (EC) 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ (L 178) 1-16 [hereinafter eCommerce Directive] Art 15; The Digital Millennium Copyright Act of 1998, 17 USC § 512(m) (United States) [hereinafter DMCA].

2 See eg eCommerce Directive (n 1) Art 12-15; DMCA (n 1) § 512(c)(1)(A-C).

monitoring obligations" rule set up a negligence-based intermediary liability system. Online hosting providers may become liable only if they do not take down allegedly infringing materials promptly enough upon knowledge of their existence, usually given by a notice from interested third-parties.[3] Although imperfect because of considerable chilling effects,[4] a negligence-based intermediary liability system has inherent built-in protections for fundamental rights. The European Court of Justice has confirmed multiple times—at least with regard to copyright infringement—that there is no room for proactive monitoring and filtering mechanisms under EU law.[5] Again, the Joint Declaration of the Three Special Rapporteurs on Freedom of Expression calls against the imposition of duties to monitor the legality of the activity taking place within the intermediaries' services.[6]

3 However, rumor has it that the principle of "no monitoring obligations"—and the negligence-based system it propels—might be in great danger, if it has not been killed off already. A fundamental tenet of online intermediaries' governance has been increasingly challenged.[7] Who killed—or is trying to kill—"no monitoring obligations"? And why? The predicament in which the principle of no proactive monitoring finds itself is the result of miscellaneous concomitant factors and spans all subject matters relevant to intermediary liability online. In search of the culprit, this paper will investigate recent case law, law reform, and private ordering.[8]

B. Untameable Monsters, Internet Threats and Value Gaps

4 As mentioned, this is a story of untameable monsters. These monsters have recently been seen in Brazil, apparently in the proximities of the Brazilian *Superior Tribunal de Justiça* (STJ). In imposing a strict liability regime for alleged copyright infringement occurring on YouTube, Justice Luis Felipe Salomão of the Brazilian STJ stated that "if Google created an 'untameable monster,' it should be the only one charged with any disastrous consequences generated by the lack of control of the users of its websites."[9] As per Justice Salomão's metaphor, the dangers for "no monitoring obligations" might follow as reaction to a fear for technological innovation that has posed unprecedented challenges to semiotic governance.

5 By evoking the untamable monster, Justice Salomão echoes a recurrent narrative in recent intermediary liability—especially copyright—policy. This narrative has focused on the "threat" posed by digitalisation and internet distribution.[10] It has led to overreaching expansion of online enforcement. The Court in *Dafra* stressed the importance of imposing liability on intermediaries, stating that "violations of privacy of individuals and companies, summary trials and

3 Please consider that there is no direct relation between liability and exemptions, which function as an extra layer of protection intended to harmonize at the EU level conditions to limit intermediary liability.

4 See e.g. Wendy Seltzer, 'Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment' (2010) 24 Harv J L & Tech 171, 175–76; Center For Democracy & Technology, Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech 1-19 (September 2010). There is abundant empirical evidence of "over-removal" by internet hosting providers. See eg Althaf Marsoof, 'Notice and Takedown: A Copyright Perspective' (2015) 5(2) Queen Mary J of Intell Prop 183, 183-205; Daniel Seng, 'The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices' (2014) 18 Va J L & Tech 369; Jennifer Urban and Laura Quilter, 'Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act' (2006) 22 Santa Clara Comp and High Tech L J 621; Lumen <www.lumendatabase.org> (formerly Chilling Effects—archiving takedown notices to promote transparency and facilitate research about the takedown ecology). However, recent U.S. caselaw gave some breathing space to UGC creators from bogus takedown notices in cases of blatant misrepresentation of fair use defences by copyright holders. See Stephanie Lenz v. Universal Music Corp, 801 F.3d 1126, 1131 (9th Cir 2015) (holding that "the statute requires copyright holders to consider fair use before sending takedown notifications").

5 See Case C-70/10 Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) [2011] ECLI:EU:C:2011:771 (re-stating the principles in favour of access providers); C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV* [2012] ECLI:EU:C:2012:85 (confirming the principle in favour of hosting providers).

6 See Joint Declaration of the Three Special Rapporteurs for Freedom of Expression (2011) 2.b. <http://www.osce.org/fom/78309?download =true>.

7 See Giancarlo Frosio, 'From Horizontal to Vertical: An Intermediary Liability Earthquake in Europe' (2017) 12 Oxford JIPLP (published online on 12 May) <https://doi.org/10.1093/jiplp/jpx061> (discussing a move from a negligence-based to a strict liability approach in recent proposals).

8 Please consider that this paper has chosen to give special emphasis to the review of case law on point. Private ordering and legislative proposals are described in lesser detail, both for reasons of space and because they have been the focus of other recent pieces from this author. See Frosio (n 7) (discussing filtering monitoring reform proposals); Giancarlo Frosio, 'Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy' (2017a) 112 Northwestern U L Rev 19 (2017) (discussing reform proposals); Giancarlo Frosio, 'Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility' (2017b) <https://papers.ssrn.com/ abstract=2976023> (discussing private ordering).

9 Google Brazil v Dafra, Special Appeal No. 1306157/SP (Superior Court of Justice, Fourth Panel, 24 March 2014) <https://cyberlaw.stanford.edu/page/wilmap-brazil>.

10 See James Boyle, The Public Domain: Enclosing the Commons of the Mind (Yale University Press 2008) 54-82.

public lynching of innocents are routinely reported, all practiced in the worldwide web with substantially increased damage because of the widespread nature of this medium of expression."[11] A paradigmatic example of the "internet threat" discourse is Justice Newman's statement in *Universal v Corley*. Responding to the requests of the defendants not to use the Digital Millennium Copyright Act (DMCA) as an instrument of censorship, Justice Newman from the United States Court of Appeal of the Second Circuit replied: "[h]ere, dissemination itself carries very substantial risk of imminent harm because the mechanism is so unusual by which dissemination of means of circumventing access controls to copyrighted works threatens to produce virtually unstoppable infringement of copyright."[12] In another landmark case, which recently appeared before the European Court of Human Rights (ECHR), the "Internet threat" discourse resurfaced again to impose proactive monitoring obligation on online news portals. This time discussing hate speech, rather than copyright infringement, the ECHR noted that in the Internet, "[d]efamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online."[13]

6 More recently, untameable monsters and Internet threats—perhaps of an imaginary type—have been evoked to justify the upcoming European copyright reform in the Digital Single Market and the introduction of filtering obligations for online intermediaries. The proposal for a Directive on Copyright in the Digital Single Market aims—*inter alia*—to close the so-called 'value gap' between Internet platforms and copyright holders.[14] Calling for a fairer allocation of value generated by the online distribution of copyright-protected content by online platforms,[15] the Communication on Online Platforms and the Digital Single Market noted that rebalancing is needed because "new forms of online content distribution have emerged [...] that may make copyright protected content uploaded by end-users widely available."[16] The idea of a 'value gap' echoes a discourse almost exclusively fabricated by the music and entertainment industry,[17] which appears to be scarcely concerned with empirical evidence. The European Copyright Society stressed this point by noting: 'we are disappointed to see that the proposals are not grounded in any solid scientific (in particular, economic) evidence."[18] Actually, the Draft Directive's Impact Assessment itself admits lack of empirical support quite plainly by noting that "the limited availability of data in this area [. . .] did not allow to elaborate a quantitative analysis of the impacts of the different policy options."[19] Moreover, a Report commissioned by the European Commission—and delivered in May 2015 but released only recently following an access to document request from a Pirate Party's MEP[20]—showed that there is actually no "robust statistical evidence of displacement of sales by online copyright infringements."[21] In sum, reform and enforcement expansion is based on unfounded assumptions. In contrast, the literature has shown to a certain degree of consistency that there is in fact an added value to promote, rather than a value gap to close.[22] Overlooking this empirical evidence—or at least moving forward without an impact statement that would consider all evidence and possible narratives—does characterize the reform as a reactionary measure to volatile fears

11 Dafra (n 9) § 5.4.

12 Universal v Corley, 273 F.3d 429, 60 U.S.P.Q.2d 1953, 1968 (2nd Cir. 2001).

13 *Delfi AS v. Estonia* N 64569/09 (ECHR, 16 June 2015) § 110.

14 Commission, 'Proposal for a Council Directive on Copyright in the Digital Single Market' COM (2016) 593 final, art 13.

15 Communication from the Commission to the European Parliament, the Council, and the Economic and Social Committee, and the Committee of the Regions, Online Platforms and the Digital Single Market: Opportunities and Challenges for Europe, COM(2016) 288 Final (May 25, 2016) 9.

16 *Id.*

17 See Martin Husovec, 'EC Proposes Stay-down & Expanded Obligation to Licence UGC Services' (*Hut'ko's Technology Law Blog*, 1 September 2016) <http://www.husovec.eu/2016/09/ec-proposes-stay-down-expanded.html>.

18 European Copyright Society, General Opinion on the EU Copyright Reform Package (24 January 2017) 5.

19 Commission, 'Staff Working Document, Impact Assessment on the Modernisation of EU Copyright Rules' SWD (2016) 301 final, PART 1/3, p 136. In general, there is no clear evidence on the effects of copyright infringement in the digital environment, the scale of it, the nature of it, or the effectiveness of more aggressive enforcement strategies. See Ian Hargreaves, 'Digital Opportunity. A Review of Intellectual Property and Growth' (May 2011) 10. See also Joe Karaganis, 'Rethinking Piracy', in Joe Karaganis (ed), *Media Piracy in Emerging Economies* (Social Science Research Center 2011) 4-11 (making the same point).

20 See Julia Reda, What the Commission Found Out About Copyright Infringement but 'Forgot' to Tell Us, (JuliaReda.eu, 20 September 2017) <https://juliareda.eu/2017/09/secret-copyright-infringement-study>.

21 Martin van der Ende, Joost Poort, Robert Haffner, Patrick de Bas, Anastasia Yagafarova, Sophie Rohlfs, Harry van Til, *Estimating Displacement Rates of Copyrighted Content in the EU: Final Report*, European Commission, May 2015, 7.

22 See, for an extended review of the literature proving this point, Giancarlo Frosio, 'Digital Piracy Debunked: A Short Note on Digital Threats and Intermediary Liability' (2016) 5(1) Internet Policy Review 1-22 <http://policyreview.info/articles/analysis/digital-piracy-debunked-short-note-digital-threats-and-intermediary-liability>. See also eg Michael Masnick and Michael Ho, The Sky is Rising: A Detailed Look at the State of the Entertainment Industry (Floor 64, January 2012), <http://www.techdirt.com/skyisrising>; Joel Waldfogel, 'Is the Sky Falling? The Quality of New Recorded Music Since Napster' (VOX, 14 November 2011) <http://www.voxeu.org/index.php?q=node/ 7274>.

based on a moral approach rather than a welfare cost/benefit analysis.[23]

C. Private Ordering

7 Filtering and proactive monitoring have been increasingly sought—and deployed—as enforcement strategies online. Proactive monitoring comes first—and largely—as a private ordering approach following rightholders and government pressures to purge the Internet from allegedly infringing content or illegal speech. In the midst of major lawsuits launched against them,[24] YouTube and Vimeo felt compelled to implement filtering mechanisms on their platforms on a voluntary basis. Google lunched Contend ID in 2008.[25] Vimeo adopted Copyright Match in 2014.[26] Both technologies rely on digital fingerprinting to match an uploaded file against a database of protected works provided by rightholders.[27] Google's Content ID—but Copyright Match works similarly—applies four possible policies, including (1) muting matched audio in an uploaded video, (2) completely blocking a matched video, (3) monetizing a matched video for the copyright owner by running advertisement against it, and (4) tracking a match video's viewership statistics.[28] Tailoring of Contend ID policies is also possible and rightholders can block content in some instances and monetize in others, depending on the amount of copyrighted content included in the allegedly infringing uploaded file. The system also allows end-users to dispute copyright owners' claims on content.[29]

8 The promotion of private ordering is a strategy increasingly adopted by governments as—in Europe for example—it would allow to circumvent the EU Charter on restrictions to fundamental rights and avoid the threat of legal challenges.[30] The *Communication on Online Platforms and the Digital Single Market* puts forward the idea that "the responsibility of online platforms is a key and cross-cutting issue."[31] Again, few months later, in its most recent Communication, the Commission made this goal even clearer by openly pursuing 'enhanced responsibility of online platforms' on a voluntary basis.[32] In other words, the Commission would like to impose an obligation on online platforms to behave responsibly by addressing specific problems.[33] Online platforms would be invested by a duty to 'ensure a safe online environment' against illegal activities.[34] Hosting providers—especially platforms—would be called to actively and swiftly remove illegal materials, instead of reacting to complaints. They would be called to adopt effective voluntary '*proactive* measures to detect and remove illegal content online'[35] and are encouraged to do so by using automatic detection and filtering technologies.[36] As the Commission puts it, the goal is "to engage with platforms in setting up and applying voluntary cooperation mechanisms" [37], in particular by setting up a privileged channel with 'trusted flaggers', competent authorities and specialized private entities with specific expertise in identifying illegal content'.[38]

9 The adoption of voluntary filtering measures does expand beyond intellectual property enforcement to reach speech-related crimes. "Online platforms must be encouraged to take more effective voluntary action to curtail exposure to illegal or harmful content" such as incitement to terrorism, child sexual abuse and hate speech.[39] As an umbrella framework, the Commission recently agreed with all major online hosting providers—including Facebook, Twitter, YouTube and Microsoft—on a code of conduct that includes a series of commitments to combat the spread of illegal hate speech online in Europe.[40] Also, in partial response

23 See Frosio (n 8) 3-12.

24 See Viacom Int'l v. YouTube Inc 676 F3d 19 (2nd Cir 2012) (upholding YouTube's liability in the long lasting legal battle with Viacom by holding that Google and YouTube had actual knowledge or awareness of specific infringing activity on its website); Capitol Records LLC v. Vimeo 972 F Supp 2d 500 (SDNY 2013) (denying in part Vimeo's motion for summary judgment).

25 See YouTube, How Content ID Works <https://support.google.com/youtube/answer/2797370?hl=en>.

26 See Chris Welch, 'Vimeo Rolls Out Copyright Match to Find and Remove Illegal Videos' (*The Verge*, 21 May 2014) <https://www.theverge.com/2014/5/21/5738584/vimeo-copyright-match-finds-and-removes-illegal-videos>.

27 See YouTube (n 25).

28 ibid.

29 YouTube, Dispute a Content ID Claim <https://support.google.com/youtube/answer/2797454?hl=en>.

30 See, for an overview of private ordering strategies. Frosio (n 23).

31 Communication (n 15) 9.

32 See Communication from the Commission to the European Parliament, the Council, and the Economic and Social Committee, and the Committee of the Regions, Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms, COM(2017)555final (September 28, 2017).

33 See Communication (n 15) 8.

34 Communication (32) § 3.

35 ibid § 3.3.1 (noting that adopting such voluntary proactive measures does not lead the online platform to automatically lose the hosting liability exemption provided by the eCommerce Directive

36 ibid § 3.3.2.

37 Communication (n 15) 8.

38 See Communication (32) § 3.2.1.

39 Communication (n 15) 9. See also Communication (32) § 1-2.

40 See Commission, European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech, Press Release (31 May 2016) <http://europa.eu/rapid/press-release_IP-16-1937_en.htm>.

to this increased pressure from the EU regarding the role of intermediaries in the fight against online terrorism, major tech companies announced that they will begin sharing hashes of apparent terrorist propaganda.[41] For some time, YouTube and Facebook have been using ContentID and other matching tools to filter "extremist content."[42] In this context, tech companies plan to create a shared database of unique digital fingerprints—knows as hashes—that can identify images and videos promoting terrorism.[43] This could include recruitment videos or violent terrorist imagery or memes. When one company identifies and removes such a piece of content, the others will be able to use the hash to identify and remove the same piece of content from their own network. The fingerprints will help identify image and video content that are "most likely to violate all of our respective companies' content policies".[44] Despite the collaboration, the task of defining removal policies will remain within the remit of each platform.[45]

D. Case Law

10 As mentioned, voluntary monitoring and filtering schemes emerged as a response to major lawsuits threatening online intermediaries. In fact, private ordering confirms a trend in recent intermediary liability policy that surfaced consistently in judicial decisions.[46] In multiple jurisdictions, case law has imposed proactive monitor obligations on online intermediaries for copyright infringement. However, proactive monitoring obligations have been spanning the entire spectrum of intermediary liability subject matters: intellectual property, privacy, defamation, and hate/dangerous speech.

11 Proactive monitoring obligations have been applied by courts on the basis of miscellaneous doctrines attempting to impose strict liability rather than negligence-based standards to intermediaries.[47] In Europe, for example, the eCommerce Directive also contains a provision that dilutes the notice-and-take-down principle by extending in specific circumstances liability beyond the liability upon knowledge. According to Art. 14(3) further obligations can be imposed by court or authority orders "requiring the service provider to terminate and prevent an infringement."[48] In this respect, the eCommerce Directive prohibits *general* monitoring obligations, although it does allow national law to provide for monitoring obligations "in a specific case."[49] The eCommerce Directive also acknowledges that Member States can impose duties of care on hosting providers "in order to detect and prevent certain types of illegal activities."[50] However, their scope should not extend to general monitoring obligations, if any meaning should be given to the previous statement in Recital 47 that only specific monitoring obligations are allowed. Moreover, the Directive states that duties of care should "*reasonably* be expected from the service providers," and no general monitoring obligation can fulfill such an expectation as they are explicitly barred by the Directive itself.[51] In order to distinguish general from specific monitoring obligations, it should be considered that (1) as an exception, specific monitoring obligations must be interpreted narrowly, (2) both the scope of the possible infringements and the amount of infringements that can be reasonably expected to be identified, must be sufficiently narrow, and (3) it must be obvious which materials constitute an infringement.[52] As Van Eecke noted

> *[i]f [clear criteria] are not defined, or only vague criteria are defined by the court (e.g. "remove all illegal videos"), or if criteria are defined that would oblige the hosting provider to necessarily investigate each and every video on its systems (e.g. "remove all racist videos"), or if the service provider were required also to remove all variations in the future (e.g.*

41 See 'Google in Europe, Partnering to Help Curb the Spread of Terrorist Content Online' (*Google Blog*, 5 December 2016) <https://blog.google/topics/google-europe/partnering-help-curb-spread-terrorist-content-online>.

42 See Joseph Menn and Dustin Volz, 'Exclusive: Google, Facebook Quietly Move Toward Automatic Blocking of Extremist Videos' (*Reuters*, 25 June 2016) <http://www.reuters.com/article/us-internet-extremism-video-exclusive-idUSKCN0ZB00M> (apparently, the "automatic" removal of extremist content is only about automatically identifying duplicate copies of video that were already removed through human review).

43 Olivia Solon, 'Facebook, Twitter, Google and Microsoft Team up to Tackle Extremist Content (*The Guardian,* 6 December 2016) <https://www.theguardian.com/technology/2016/dec/05/facebook-twitter-google-microsoft-terrorist-extremist-content>.

44 See 'Partnering to Help Curb Spread of Online Terrorist Content' (*Facebook Newsroom*, 5 December 2016) <https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content>.

45 ibid.

46 *See*, for full reference, summaries in English and links to most decision cited in the next few pages, The World Intermediary Liability Map (WILMap), <http://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap> (a project designed and developed by Giancarlo Frosio and hosted at Stanford CIS).

47 See Broder Kleinschmidt, 'An International Comparison of ISP's Liabilities for Unlawful Third Party Content' (2010) 18(4) IJLIT 332, 346-347.

48 See eCommerce Directive (n 2) Art. 14(3).

49 ibid Recital 47.

50 ibid Recital 48.

51 ibid (emphasis added).

52 See Patrick Van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach' (2011) 48(5) Common Market L Rev 1455, 1486-1487.

"remove this video, but also all other videos that belong to the same repertory"), a general monitoring obligation would be imposed.[53]

12 Although space limitation necessary constricts the scope of this review, this section will select several cases in multiple jurisdictions where monitoring obligations have been imposed. As said, this case law deals with the entire variety of potential infringements that may trigger online intermediary liability, proving that—also at the judicial level—the emergence of proactive monitoring obligations is a global intermediary liability policy trend. However, notable exceptions to this emerging trend—such as the landmark Belen case in Argentina—will also be considered.

I. Copyright: From Dafra to Baidu

13 Multiple judicial decisions have imposed proactive monitoring obligations for copyright infringement on hosting providers. Let us start by going back to the beginning of our story then. As mentioned earlier, the Brazilian STJ imposed proactive monitoring obligations on YouTube.[54] The Brazilian STJ found Google liable for copyright infringement for YouTube-hosted videos parodying a well-known commercial.[55] As such, Dafra stands as a perfect case study regarding the effects of filtering on freedom of expression online. Dafra is a motorcycle manufacturer, which broadcasted a commercial titled "Meetings," as part of a national advertising campaign known as "Dafra – You on Top."[56] Shortly after launching the advertising campaign, a YouTube user published a "fan-dub" of the original Dafra video.[57] In the user-generated parody version of Dafra's commercial, the actor's original voice was replaced by a very similar one making statements tarnishing Dafra's goodwill.[58] Google took down the initial video per Dafra's request, but several other versions of the video were posted constantly by other users under different titles.[59] Therefore, Dafra sued Google for copyright infringement, claiming that Google had not adopted the necessary measures to avoid further viewing of videos with the same content, regardless of the title that users may have given to those videos.[60] The plaintiff had asked Google not only to remove the video but also to use search blocking mechanisms to prevent posting any unauthorized material related to the "Dafra – You on Top" campaign on YouTube.[61]

14 The STJ upheld the plaintiff's claims for copyright infringement and ordered Google to remove all the adulterated advertisements within 24 hours, under a penalty of R$ 500 per day for noncompliance.[62] According to the decision, Google must remove not only the infringing video, which is the object of the lawsuit, but also any similar and related unauthorized videos, even if they are uploaded by other users and bear a different title.[63] However, the Court recognized "certain limitations of proactive control."[64] The judgment does not address future videos and Google's obligation only reaches unauthorized videos with "Dafra – You on Top" in the title.[65] In fact, Google claimed a "technical impossibility" defense, arguing that it was impossible to take down all videos because there are currently no blocking filters able to identify all infringing materials.[66] Justice Salomão—the rapporteur of the case—quashed Google's "technical impossibility defense" because lack of technical solutions for fixing a defective new product does not exempt the manufacturer from liability, or from the obligation of providing a solution.[67] If Google created an 'untamable monster,'—Justice Salomão continued—"it should be the only one charged with any disastrous consequences generated by the lack of control of the users of its websites."[68]

15 *Dafra* is not an isolated case. Recently, several European national decisions implemented proactive monitoring obligations for hosting providers in apparent conflict with a well settled jurisprudence of the CJEU. In *Allostreaming*—a landmark case in France—the Paris Court of Appeal confirmed in part a previous decision of the *Tribunal de Grande Instance*.[69] The Court imposed on access providers

53 ibid 1487.

54 See Dafra (n 9). See also Giancarlo Frosio, 'Brazilian Supreme Court Found Google Liable for Videos Parodying Dafra's Commercials' (*CIS Blog*, 31 January 2014) <https://cyberlaw.stanford.edu/blog/2014/01/brazilian-supreme-court-found-google-liable-videos-parodying-dafra%E2%80%99s-commercials>.

55 See Dafra (n 9) § 1.

56 ibid.

57 ibid.

58 ibid. See also YouTube, This video is unavailable <https://www.youtube.com/watch?v=luu_73y_hCk>.

59 See Dafra (n 9) § 1.

60 ibid.

61 ibid.

62 ibid § 8.

63 ibid § 5.2.

64 ibid.

65 ibid.

66 ibid § 4.

67 ibid § 5.4

68 ibid.

69 See APC et al v. Google, Microsoft, Yahoo!, Bouygues et Al (Cour d'Appel Paris, 16 March 2016) (France) [hereinafter Allostreaming 2016] confirming APC et al v. Google, Microsoft, Yahoo!, Bouygues et Al (TGI Paris, 28 November 2013) (France). See also Laura Marino, 'Responsabilités civile et pénale des fournisseurs d'accès et d'hébergement' (2016) 670 JCl. Communication 71, 71-79. But see TF1 v.

an obligation to block the illegal movie streaming website Allostreaming and affiliated enterprises. In addition, search engines, including Google, Yahoo! and Bing, are obliged to proactively expunge their search results from any link to the same websites.[70] Notably, the appellate decision reversed the first instance on the issue of costs allocation. According to the Court of Appeal, all costs related to blocking and delisting sixteen Allostreaming websites should be sustained by the search engines, rather than being equally shared as previously decided.[71] As to be considered later, the stand taken by the Paris Court of Appeal has obvious implications in regard to the inadequate balance with freedom to conduct business that monitoring obligations might bring about as discussed multiple times by the CJEU. In laying down its arguments for proactive monitoring and cost allocation, *Allostreaming* also evokes the specter of the untamable monster. The Court remarked that rightholders are "confronted with a massive attack" and are "heavily threatened by the massive piracy of their works."[72] Hence, the Court continues, it is "legitimate and in accordance with the principle of proportionality that [ISPs and search engines] contribute to blocking and delisting measures" because they "initiate the activity of making available access to these websites" and "derive economic benefit from this access (especially by advertising displayed on their pages)."[73] Regardless the logic of the argument, proactive monitoring and imposition of liability to innocent third parties is apparently still upheld by endorsing an Internet threat discourse.

16 Under the Telemedia Act, German courts found that host providers are ineligible for the liability privilege if their business model is mainly based on copyright infringement. In two disputes involving the Swiss-based file-hosting service, RapidShare, the Bundesgerichtshof (German Supreme Court) imposed monitoring obligations on RapidShare.[74] According to the Court, although RapidShare's business model is not primarily designed for violating rights, it nevertheless provides incentives to third parties to illegally share copyrighted content.[75] Therefore, as the Bundesgerichtshof also announced in Atari Europe v. RapidShare,[76] RapidShare—and similar file-hosting services—should abide to more stringent monitoring duties.[77] According to the Court, a hosting provider is not only required to delete files containing copyrighted material as soon as it is notified of a violation by the right holder, but must also take steps to prevent similar infringements by other users in the future.[78] File-hosting services are required to actively monitor incoming links to discover copyrighted files as soon as there is a specific reason to do so and to then ensure that these files become inaccessible to the public.[79] As indicated by the Court, the service provider should use all possible resources - including search engines, Facebook, Twitter, or web crawlers - to identify links made accessible to the public by user generated repositories of links.[80]

17 In Italy, a mixed case law emerged. Some courts imposed proactive monitoring obligations on intermediaries, whereas other courts took the opposite stance and confirmed that there is no monitoring obligation for intermediaries under European law.[81] There is a long-lasting legal battle between Delta TV and YouTube being fought before

DailyMotion (Cour d'Appel Paris, 2 December 2014) (stating that DailyMotion enjoys limitation of liability as a hosting provider and is not required to proactively monitor users' infringing activities). See also Giancarlo Frosio, 'France DailyMotion pays Damages for Late Removal of Infringing Materials' (*CIS Blog*, 8 December 2014) <https://cyberlaw.stanford.edu/blog/2014/12/france-dailymotion-pays-damages-late-removal-infringing-materials>.

70 See Allostreaming 2016 (n 69) 7.

71 ibid 42.

72 ibid.

73 ibid

74 See GEMA v RapidShare I ZR 79/12 (Bundesgerichtshof, August 15, 2013) (Germany) (where the German copyright collective society, GEMA, sued RapidShare in Germany, alleging that over 4,800 copyrighted music files were shared via RapidShare without consent from GEMA or the right holder). An English translation is here: <https://stichtingbrein.nl/public/2013-08-15%20BGH_RapidShare_EN.pdf>.

75 ibid.

76 See Atari Europe v. RapidShare I ZR 18/11 (Bundesgerichtshof, July 12, 2012) (Germany) (in this case, RapidShare neglected to check whether certain files violating Atari's copyright over the computer game "Alone in the dark" were stored on its servers by other users).

77 See GEMA v. RapidShare (n 74); Atari Europe v. RapidShare (n 76).

78 ibid.

79 See GEMA v. RapidShare (n 74) § 60.

80 ibid.

81 For case law confirming the safe harbour and no-monitoring obligations, see Reti Televisive Italiane S.p.A. (RTI) v. Yahoo! Italia S.r.l. (Yahoo!) et al, N RG 3821/2011 (Milan Court of Appeal, 7 January 2015) (reversing a previous decision regarding the publication of fragments of television programs through the now-terminated Yahoo! Video service and clarified that RTI had the obligation to indicate in a "detailed, precise and specific manner" the videos that Yahoo! had to remove and the court of first instance could not "impose to a hosting provider general orders or, even worse, general monitoring obligations, which are forbidden by Directive 2000/31/EC"); Mediaset Premium S.p.a. v. Telecom Italia S.p.a. et al (Milan Tribunal, 27 July 2016) (discussing a blocking injunction against Calcion. at and clarifying that mere conduit internet providers do not have an obligation to monitor their networks and automatically remove content). See also Reti Televisive Italiane S.p.A. (RTI) v. TMFT Enterprises LLC- Break Media, (Rome Tribunal, 27 April 2016) (confirming no monitoring obligations but stating that rightholders do not need to list the URLs where the videos are made available).

the Tribunal of Turin. Delta TV sued Google and YouTube for copyright infringement of certain South American soap operas that users had uploaded to YouTube. In this case, Google complied with its notice-and-take-down policy, and the videos were removed as soon as the specific URLs were provided by Delta TV. In one interim decision, the Court agreed with Delta TV's claims and ordered Google and YouTube to remove the infringing videos and to prevent further uploads of the same content through the use of its Content ID software using as a reference the URLs provided by Delta TV.[82] The Court stressed that these proactive monitoring obligations derive from the fact that YouTube is a "new generation" hosting service, a role that brought on it a greater responsibility to protect third parties' rights.[83] More recently, the Tribunal of Turin delivered a final decision on the matter, confirming the previous decision and an obligation for YouTube to partially monitor its network by preventing the re-uploading of content previously removed.[84] The Court noted that "there subsists on YouTube an actual legal obligation to prevent further uploads of videos already flagged as infringing of third-party copyrights."[85] This would be—according to the Court—an *ex post* specific obligation or duty of care in line with Recital 40 of the eCommerce Directive. It is worth noting that multiple Italian cases applied a reasoning similar to that of the Brazilian STJ in *Dafra*, by stating that any hosting providers, whether active or passive, have an obligation to prevent the repetition of further infringements once they have actual knowledge of the infringement, according to the principle *cuius commoda, eius et incommoda* ("a party enjoying the benefits [of an activity] should bear also the inconveniences").[86] This civil law principle refers to a form of extra-contractual (or tort) liability for which whoever benefits from a certain activity should be liable for any damages that such activity may cause.

18 In China, the Beijing Higher People's Court developed an interesting standard for proactive monitoring. In the *Baidu* case, the Court set up a duty to monitor for hosting providers based on popularity of infringed works and high-volume views/downloads.[87] The plaintiff Zhong Qin Wen found his copyrighted works—in particular the short book *English Learning Diary of Koala Xiaowu – to Those Fighting for Their Dreams* (《考拉小巫的英语学习日记——写给为梦想而奋斗的人》)—made available on the platform BaiduWenku and sued Baidu for copyright infringement.[88] According to the High Court of Beijing, by using current technologies, it was reasonable for Baidu to exercise a duty to monitor and examine the legal status of an uploaded work once it has been viewed or downloaded more than a certain number of times.[89] According to the Court, Baidu needs to inspect the potential copyright status of the work by contacting the uploader, checking whether the work is originally created by the uploader or legally authorized by the copyright owners.[90] Apparently, this case sets a duty for Internet hosting providers to protect popular works that attract many views and downloads. However, both Beijing First Immediate People's Court and Beijing Higher People's Court failed to set a clear indication of how many views or downloads are enough to trigger the duty, thus making uncertain intermediaries' proactive monitoring obligations.[91]

Belen Rodriguez and Beyond: Exceptions to an Emerging Global Trend

19 Notable exceptions to this trend in enforcing proacting monitoring obligations highlight, however, some fragmentation in the international response to intermediary liability. A recent landmark case decided by the Argentinian Supreme Court rejected any filtering obligation to prevent infringing links from appearing in search engines' results in the future.[92] The case was brought forward by a well-

82 *See* Delta TV v Youtube, N RG 15218/2014 (Tribunal of Turin, 23 June 2014) (revising en banc a previous decision rejecting Delta TV's request on the basis that (i) there is no obligation on the part of Google and YouTube, as hosting providers, to assess the actual ownership of the copyrights in videos uploaded by individual users). See also Eleonora Rosati, 'Italian court says that YouTube's Content ID should be used to block allegedly infringing contents' (*IPKat*, 21 July 2014) <http://ipkitten.blogspot.fr/2014/07/italian-court-says-that-youtubes.html>.

83 ibid 12.

84 See Delta TV v Google and YouTube, N RG 38113/2013 (Turin Tribunal, 7 April 2017).

85 Eleonora Rosati, 'Italian court finds Google and YouTube liable for failing to remove unlicensed content (but confirms eligibility for safe harbour protection)' (*IPKat*, 30 April 2017) <http://ipkitten.blogspot.fr/2017/04/italian-court-finds-google-and-youtube.html>.

86 See eg David Drummond et al, N 1972/2010 (Milan Tribunal, Criminal Section, 16 April 2013) <http://speciali.espresso.repubblica.it//pdf/Motivazioni_sentenza_Google.pdf> (discussing the notorious Vividown case and convicting Google executives for violating data protection law, in connection with the online posting of a video showing a disabled person being bullied and insulted). See also Giovanni Sartor and Mario Viola de Azevedo Cunha, 'The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents' (2010) 18(4) Int J law Info Tech 356, 373-374.

87 See Zhong Qin Wen v Baidu, 2014 Gao Min Zhong Zi, No. 2045 (Beijing Higher People's Court 2014) <https://cyberlaw.stanford.edu/page/wilmap-china>.

88 ibid.

89 ibid.

90 ibid.

91 ibid.

92 Rodriguez M. Belen c/Google y Otro s/ daños y perjuicios, R.522.XLIX. (Supreme Court, October 29, 2014) (Argentina). See also Pablo Palazzi and Marco Jurado, 'Search Engine Liability for Third Party Infringement' (2015) 10(4) JIPLP

known public figure—Belen Rodriguez—for violation of her copyright, reputation and privacy.[93] This case is one among numerous civil lawsuits brought against the search engines Google and Yahoo! by different 'celebrities' and well-known public figures for violation of their reputation and privacy.[94] The case discussed the question whether search engines are liable for linking in search results to third-party content that violates fundamental rights or infringes copyright. Initially, some lower courts found search engines strictly liable under Article 1113 of the Civil Code, which imposes liability, regardless of knowledge or intention, to those performing risky acts, such as indexing third party content creating wider audiences for illegitimate content, or serving as the "guardians" of the element that generates the damage, such as the search engine's software.[95] Finally, the Argentinian Supreme Court: (1) repudiated a strict liability standard and adopted a test based on actual knowledge and negligence; (2) requested judicial review for issuing a notice to take down content—except in a few cases of "gross and manifest harm"; and (3) rejected any filtering obligation to prevent infringing links from appearing in the future.[96] In the rather extreme view taken by the Argentinian Supreme Court, as a default rule, actual knowledge—and possibly negligence—would only arise after a judicial review has upheld the issuance of the notice. In any event, this conclusion—and the transaction costs that brings about—is mitigated by a category of cases exempted from judicial review that might finally be quite substantial. Apparently, the Argentinian Supreme Court believes that, if harm is not manifest, a balancing of rights might be necessary, which can be done only by a court of law, rather than a private party.

20 Indeed, multiple national decisions in Europe have denied the applications of monitoring obligations in application of the eCommerce Directive legal framework. Mixed approaches apparent in the Italian courts have been mentioned earlier. A good example of the court's rationale in these cases can be found in one of the Telecinco cases in Spain. The Madrid Court of Appeal dismissed the request of Telecinco—a Spanish broadcaster owned by the Italian Mediaset—to issue an injunction towards potential future infringements on YouTube. The Spanish Court laid out a set of arguments showing how European law and jurisprudence would pre-empt proactive monitoring at the national level. Although the CJEU interpreted Article 11 of the Enforcement Directive as meaning that an ISP may be ordered "to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of that kind,"[97] the Madrid Court said, it also made clear that this rule "may not affect the provisions of Directive 2000/31 and, more specifically, Articles 12 to 15 thereof ... which prohibits national authorities from adopting measures which would require a hosting service provider to carry out general monitoring of the information that it stores."[98]A possible injunction against future infringements—the Court of Appeal concluded—would result either in an order to monitor UGCs proactively, contrary to the E-Commerce Directive, or in an obligation to implement a filtering system that, according to the CJEU, would seriously endanger ISPs' freedoms to conduct business and users' fundamental rights, including data protection and freedom of information.[99]

II. Trademark: The Internet Auction Cases

21 Proactive monitoring does not only emerge in copyright enforcement. Trademark enforcement has seen courts imposing upon intermediaries similar obligations.[100] In a series of landmark decisions, the German Federal Court of Justice—*Bundesgerichtshof*—imposed supplementary duties on host providers in addition to notice-and-takedown obligations.[101] A

244; Marco Rizzo Jurado, 'Search engine liability arising from third parties infringing content: a path to strict liability?' (2014) 9(9) JIPLP 718, 718-720.

93 See Belen (n 92).

94 See eg S. M., M. S. c/ Yahoo de Argentina SRL y Otro s/ daños y perjuicios, N 89.007/2006; AR/JUR/XXXXX/2013 (Cámara Nacional de Apelaciones en lo Civil de la Capital Federal, 6 November 2013); Da Cunha, Virginia c. Yahoo de Argentina S.R.L. and Google, N 99.620/2006, AR/JUR/40066/2010 (Cámara Nacional de Apelaciones en lo Civil de la Capital Federal, 10 August 2010).

95 See eg Yahoo (n 94).

96 See Belen (n 92).

97 C-324/09 *L'Oréal SA and Others v. eBay International AG and Others* (2012) § 144.

98 See C-360/10 (n 5) § 32-33; C-324/09 (n 97) § 139.

99 ibid § 48.

100 See, for a general overview of intermediary liability for online trademark infringement, Graeme B. Dinwoodie, 'Secondary Liability for Online Trademark Infringement: The International Landscape' (2014) 37 Colum J L & Arts 463; Barton Beebe, 'Tiffany and Rosetta Stone - Intermediary Liability in U.S. Trademark Law' (2012) 41 CIPA Journal 192.

101 See Rolex v Ebay/ Ricardo (a.k.a. *Internetversteigerung* I) I ZR 304/01 (BGH 11 March 2004) § 31; Rolex v. eBay (a.k.a. *Internetversteigerung* II), I ZR 35/04 (BGH, 19 April 2007) (Germany); Rolex v. Ricardo (a.k.a. *Internetversteigerung* III), Case I ZR 73/05, (BGH, 30 April 2008) (Germany). See also L'Oreal v Ebay [2009] EWHC 1094 (Ch), 455-465 <http://www.bailii.org/ew/cases/EWHC/Ch/2009/1094.html> (for an English summary of the German Federal Court's decisions regarding internet auctions); Van Eecke (n 52) 1476-1478; Anne Cheung and Kevin Pun, 'Comparative study on the liability for trade mark infringement of online auction providers' (2009) 31(11) EIPR 559, 559-567.

seller on eBay sold replica Rolex watches and posted them on eBay by using the Rolex brand. Together with trademark infringement against the primary infringer, Rolex claimed that eBay, was also liable for supplying the platform for the seller to infringe her rights.[102] In particular, Rolex sought that eBay should not only take the infringing content down, but also prevent future infringements that are similar or identical to a present infringement.[103] In the so-called Internet Auction cases I-III, the German *Bundesgerichtshof* repeatedly decided that notified trademark infringements oblige internet auction platforms such as eBay to investigate future offerings—manually or through software filters—in order to avoid further trademark infringement, if the necessary measures are possible and economically reasonable.[104]

22 The *Bundesgerichtshof* based its decision on the German doctrine of *Störerhaftung*—a property law doctrine applied by analogy to intellectual property. Actually, the same doctrine has also been applied by German courts in the *RapidShare* cases mentioned earlier and other copyright cases. According to Sec. 1004 of the German Civil Code the proprietor enjoys a right to (permanent) injunctive relief against anybody who has caused an interference with the property—so called *Störer* (interferer in English).[105] However, nobody should be held liable as a *Störer* if the duty would burden him unreasonably. The German Courts struggled with the notion of what was "technically possible" and "reasonable." The third *Internetversteigerung* case found precautions against clearly noticeable infringements reasonable, such as blatant counterfeit items.[106] In contrast, it would be unreasonable to implement a filtering obligation that questions the business model of the intermediary.[107]

23 In a later decision, the *Bundesgerichtshof* tuned down its view of reasonable precautionary means. It noted that manually checking and visually comparing each product offered in an online auction against infringement—which was not clear or obvious—would be unreasonable.[108] In particular, the Court noted that obligations are unreasonable if due to the substantial amount of products offered, the platform's business model would be endangered.[109] Offering filtering tools to trade mark holders—as eBay does—in order to perform such manual checks themselves would be apparently sufficient.[110]

III. Privacy: The Max Mosley Saga

24 The long-standing saga of Max Mosley's sexual images has offered European courts a new opportunity to strike a balance between freedom of expression and the right to privacy in light of the ubiquitous distribution power of Internet search engines. Courts in France, Germany, and the UK, imposed proactive monitoring obligations to search engines, which were ordered to expunge the Internet from pictures infringing the privacy rights of Max Mosley—former head of the *Fédération Internationale de l'Automobile*. In 2008, the *News of the World* newspaper published photos of Max Mosley engaged in sexual roleplaying with prostitutes dressed as German prison guards. The *News of the World's* headline accompanying the photos referred to a "Sick Nazi Orgy."[111] Mosley successfully sued the newspaper in the United Kingdom and later in France for breach of privacy.[112] At the same time, Mosley unsuccessfully tried to obtain a judgment from the European Court of Human Rights holding that member states should legislate under Article 8 of the European Convention of Human Rights to prevent newspapers from publishing stories regarding individuals' private lives without first warning the concerned party.[113]

25 However, the Internet is more difficult to control than traditional newspapers. Mosley's images went viral and people linked to them endlessly in cyberspace. Since then, Mosley has started a personal battle with the Internet, specifically with search engines. Mosley sued Google in several European countries, demanding that the company filter out of search results any online photos of his sexual escapade, alleging that the online publication of these images infringes Mosley's right to privacy. The Tribunal de Grande Instance in Paris recently granted Mosley's petition and ordered Google to remove from its image search, results over a period of five years that display any of the nine images Mosley identified.[114] The order required Google to implement a filter that should automatically

102 See eg *Internetversteigerung* I (n 101) § 1-5.

103 ibid.

104 ibid § 46.

105 See German Civil Code § 1004.

106 *Internetversteigerung* III (n 101).

107 ibid.

108 See (a.k.a. *Kinderhochstühle im Internet*) I ZR 139/08 (BGH, 22 July 2010) (Germany).

109 ibid.

110 ibid.

111 See, for factual background, Giancarlo Frosio, 'French Court Forces Google to Proactively Block Photographs of Sexual Escapade from Image Search' (*CIS Blog*, 21 November 2013) <https://cyberlaw.stanford.edu/blog/2013/11/french-court-forces-google-proactively-block-photographs-sexual-escapade-image-search>.

112 See *Max Mosley v. News Group Newspaper Ltd* [2008] EWHC 1777 (QB) (United Kingdom).

113 See *Mosley v. The United Kingdom* [2011] ECHR 774 (United Kingdom).

114 See *Google v. Mosley* (TGI Paris, 6 November 2013) (France).

detect pages containing the infringing photos and proactively block new versions of posted images from search results continuously.[115] As per the cost of filtering, the court noted that blocking the search results may be simple and inexpensive, and present technology, such as PhotoDNA, makes it possible to filter not only exact copies of identified images but also modified copies.[116]

26 Mosley brought a similar claim against Google in the United Kingdom under Art. 10 of the Data Protection Act 1998—the right to prevent processing likely to cause damage or distress—to oblige the search engine to disable access to pictures infringing on his privacy.[117] Google sought to strike out the claim, on the basis that the order applied for would be incompatible with Articles 13 and 15 of the eCommerce Directive.[118] However, the Court noted, first, that either with regard to the processing of personal data, the protection of individuals is governed solely by the data protection legislation[119] or, at least the two Directives must be read in harmony, giving both, if possible, full effect.[120] Whichever way, the "person whose sensitive personal data has been wrongly processed by an internet service provider [has a legal remedy to] ask the court to order it to take steps to cease to process that data."[121] The court, after noting that "is common ground that existing technology permits Google, without disproportionate effort or expense, to block access to individual images," allowed the claim to go to trial because "evidence may well satisfy a trial judge that [blocking] can be done without impermissible monitoring."[122]

27 In Germany, The District Court of Hamburg followed in the footsteps of the French and UK decisions.[123] Google was found liable as an "interferer" (*Störer)* "because it has not taken the possible and reasonable steps in accordance with the indications of the plaintiff to prevent further breaches of rights [...] and contributes willingly and causally to the violation of the protected rights."[124] According to the Court, notice-and-take-down is "insufficient for the present serious infringement."[125] Apparently, the Court deploys again the "untamable monster" argument as "[g]iven the gravity of the infringement and his efforts so far, [Mosley] is not required to take action against all the major media companies—possibly in the world—distributing these images on their own sites."[126] The Court goes on by saying that the notice of each individual infringement is only an inadequate tool "because the duty to monitor and control would provisionally remain with the plaintiff."[127] Apparently, the Court seems to forget that this is actually the goal that the eCommerce negligence-based liability arrangement would like to achieve. On Google's technical capacity to monitor, the Court believed that if software programmes like PhotoDNA, iWatch and Content-ID and image recognition software that works with so-called robust hash values, are not able to meet the requests of the plaintiff, Google should take measures to be able to prevent future harm occurring to Mosley by developing appropriate software or updating existing software that would "delete and detect or block the infringing content."[128]

IV. Defamation and Hate Speech: Delfi and its Progeny

28 In multiple decisions, the European Court of Human Rights (ECHR) had to consider whether an Internet news portal should be liable for user-generated comments and obliged to monitor and filter proactively its networks to avoid liability. In a landmark case, the Grand Chamber of ECHR confirmed the judgment previously delivered by the Fifth Section and held that finding Delfi—one of the largest news portals on the Internet in Estonia—liable for anonymous comments posted by third parties had not been in breach of its freedom to impart information.[129] In particular:

> *the case concerned the duties and responsibilities of Internet news portals which provided on a commercial basis a platform for user-generated comments on previously published content and some users – whether identified or anonymous – engaged in clearly unlawful hate speech which infringed*

115 ibid.

116 ibid.

117 See Mosley v Google [2015] EWHC 59 (QB) (United Kingdom).

118 ibid § 27-37.

119 See eCommerce Directive (n 1) Recital 14.

120 See Mosley (n 117) § 45.

121 ibid § 46.

122 ibid § 54.

123 See *Max Mosley v Google Inc.* 324 O 264/11 (Hamburg District Court, 24 January 2014) (Germany). See also Dominic Crossley, 'Hamburg District Court: Max Mosley v Google Inc, Google go down (again, this time) in Hamburg' (*Inforrm's Blog*, 5 May 2014) <https://inforrm.wordpress.com/2014/02/05/case-law-hamburg-district-court-max-mosley-v-google-inc-google-go-down-again-this-time-in-hamburg-dominic-crossley>.

124 *Mosley* (n 123) § 176 and 179.

125 ibid § 189.

126 ibid § 190.

127 ibid § 189.

128 ibid § 190 and 195.

129 See *Delfi AS* (n 13). See also eg Lisl Brunner, 'The Liability of an Online Intermediary for Third Party Content: The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia' (2016) 16(1) Human Rights L Rev 163, 163-174.

the personality rights of others.[130]

29 Delfi published an article that mentioned in its title that SLK, a company providing public ferry transportation between the mainland and some islands, "Destroyed Planned Ice Roads," which are public roads over the frozen sea.[131] Although the article was not itself defamatory, it attracted 185 comments including personal threats and offensive language directed against a member of the advisory board of SLK.[132] The target SLK board member was Jewish and several comments had a marked, and in some instances especially ignominious, anti-Semitic flare.[133] Delfi had in place a notice-and-take-down policy.[134] Upon SLK's request for removal of the comments, Delfi promptly removed the comments under its notice-and-take-down obligations.[135] However, Delfi refused SLK's additional claim for non-pecuniary damages.[136]

30 After a long-lasting legal battle in Estonian courts, the Estonian Supreme Court upheld previous judgments and reiterated that Delfi is a provider of content services,[137] rather than an information service provider, falling under the e-Commerce Directive. Delfi finally sought redress from the ECHR. The ECHR was asked to strike a balance between freedom of expression under Article 10 of the Convention and the preservation of personality rights of third persons under Article 8 of the same Convention.[138] The ECHR tackled this conundrum by delineating a narrowly construed scenario in which liability supposedly does not interfere with freedom of expression.[139] In a situation of higher-than-average risk of defamation or hate speech,[140] if comments from non-registered users are allowed,[141] a professionally managed and commercially based Internet news portal should exercise the full extent of control at its disposal—and must go beyond automatic keyword-based filtering or ex-post notice-and-take-down procedures—to avoid liability.[142] In later cases, the European Court of Human Rights has revisited—or best clarified—the issue of liability for Internet intermediaries. In *MTE*, the ECHR concluded that "the notice-and-take-down system could function in many cases as an appropriate tool for balancing the rights and interests of all those involved."[143] Therefore, if the specifics of *Delfi* do not apply and the comments to be removed are "offensive and vulgar" rather than hate speech,[144] the Court saw "no reason to hold that [the notice-and-take-down] system could not have provided a viable avenue to protect the commercial reputation of the plaintiff."[145] In this case, MTE—the Hungarian association of Internet service providers—posted an article highlighting unethical business practices by a real estate company, which prompted negative comments.[146] In Pihl v. Sweden, the ECHR confirmed the previous reasoning—and that size matters—by rejecting the claims of an applicant who had been the subject of a defamatory online comment published on a blog. The Court reasoned that no proactive monitoring *à la* Delfi was to be imposed against the defendant because although the comment had been offensive, it had not amounted to hate speech or an incitement to violence; it had been posted on a small blog run by a non-profit association; it had been taken down the day after the applicant had made a complaint; and it had only been on the blog for around nine days."

31 Still, proactive and automated monitoring and filtering—although narrowly applied—gets singled out by the ECHR as a privileged tool to tame the "untamable monster" or the "internet threat," as mentioned previously.[147] Anonymity becomes a possible representation of the "untamable monster" to be slayed, rather than a feature of online freedom of expression to be nourished.[148] Interestingly,

130 See ECHR, Press Release ECHR 205 (2015) (16 June 2015) <http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-5110487-6300958&filename=003-5110487-6300958.pdf>.

131 See *Delfi AS* (n 13) § 16.

132 ibid § 16-17.

133 ibid § 18.

134 ibid § 13-14.

135 ibid § 19.

136 ibid § 20.

137 See Delfi N 3-2-1-43-09 (*Riigikohus* [Supreme Court], 10 June 2009) (Estonia) <http://cyberlaw.stanford.edu/page/wilmap-estonia>.

138 ibid § 59.

139 See, for my detailed comments of each relevant principle stated in the decision, Giancarlo Frosio, 'The European Court Of Human Rights Holds Delfi.ee Liable For Anonymous Defamation' (*CIS Blog*, 25 October 2013) <https://cyberlaw.stanford.edu/blog/2013/10/european-court-human-rights-holds-delfiee-liable-anonymous-defamation>.

140 See *Delfi AS* (n 13) § 144-146. A strikingly similar standard was also adopted by an older decision of the Japanese Supreme Court. See Animal Hospital Case (Supreme Court, 7 October 2005) (Japan) <https://cyberlaw.stanford.edu/page/wilmap-japan> (finding Channel 2, a Japanese bulletin board, liable on the rationale that—given the large amount of defamatory and "unreliable" content in threads found on its site—it was not necessary for Channel 2 to know that each thread was defamatory, but it was sufficient that Channel 2 had the knowledge that there was a risk that such transmissions/posts could be defamatory).

141 See *Delfi AS* (n 13) § 147-151.

142 ibid § 152-159.

143 See *Magyar Tartalomszolgáltatók Egyesülete and Index.Hu v Hungary* N 22947/13 (ECHR, 2 May 2016) § 91.

144 ibid § 64.

145 ibid § 91.

146 ibid § 11.

147 See Delfi AS (n 13) § 110; infra Untameable Monsters, Internet Threats and Value Gaps.

148 See Nicolo Zingales, 'Virtues and Perils of Anonymity:

the Court seems to set a threshold for proactive monitoring based on popularity as in the *Baidu* case. Delfi—the Court noted in imposing its "higher-than-average risk" standard—could have realized that the article might have caused negative reactions because readers and commenters had a great deal of interest in the matter, as shown by the above average number of comments posted on the article.[149] In the process, over-enforcement—caused by automated filtering—challenges freedom of expression.[150] Again, the role of intermediaries is blurred with that of entities obligated to police the net for infringing activities. But is it their role?

E. Legislation

32 Legislatively mandated proactive monitoring obligations to curb online copyright infringement might soon follow in the footsteps of voluntary measures already adopted by major platforms and case law. For reasons of space, this article touches only briefly on these proposals, which nonetheless must be mentioned for sake of structural completeness. A detailed review of these proposals, however, is included in other writings of this author cited below.

33 Proactive monitoring—and filtering—sits on top of the rightsholders' wish list both in the United States and Europe.[151] In particular, a recent proposal included in the *Copyright in the Digital Single Market Draft Directive* would impose on intermediaries the implementation of effective content recognition technologies to prevent the availability of infringing content.[152] The Commission's copyright proposal would require platforms that provide access to "large amounts" of user-generated content to incorporate an automated filtering system. The proposal specifically refers to technologies such as YouTube's Content ID or other automatic infringement assessment systems.[153] Apparently, the proposal would force hosting providers to develop and deploy filtering systems, therefore *de facto* monitoring their networks.[154]

34 Proactive monitoring and filtering obligations would also find their way in European policy through an update of the audio-visual media legislation. As part of its legislative intervention package, the Commission will tackle the proliferation on online video sharing platforms of content that is harmful to minors and of hate speech with its proposal for an updated Audio-visual Media Services Directive.[155] Video hosts can be regulated like broadcasters if they step outside of their passive hosting role by organizing hosted content. The AVMS draft directive lists new obligations to remove and possibly monitor for hate speech. This specific-sector regulation would ask platforms to put in place measures to protect minors from harmful content and to protect everyone from incitement to hatred.[156] Apparently, the AVMS revision might erode the eCommerce directive's no monitoring obligations for video platforms by asking Member States to "ensure by appropriate means that audiovisual media services provided by media service providers under their jurisdiction do not contain any incitement to violence or hatred'.[157]

35 It is worth noting, however, that a heated debate is occurring in the European Parliament regarding the implementation of the Commission's proposals. Finally, the reform as approved by the Parliament might differ consistently from the proposals.[158]

Should Intermediaries Bear the Burden?' (2014) 5(3) JIPITEC 155, 155-171.

149 See Delfi AS (n 13) Joint Dissenting Opinion of Judges Sajò and Tsotsoria § I.2.

150 See Martin Husovec, 'ECHR Rules on Liability of ISPs as a Restriction of Freedom of Speech' (2014) 9(2) JIPLP 108.

151 See Joint Supplemental Comments of American Federation of Musicians et al to U.S. Copyright Office, In the Matter of Section 512 Study: Notice and Request for Public Comment, Docket No 2015-7 (28 February 2017) (the Recording Industry Association of America and 14 other groups calling for stronger regulations that would require internet service providers to block pirated content).

152 See Commission, 'Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market' COM(2016) 593 final (14 September 2016) art 13.

153 ibid.

154 I remand for a detailed analysis of this proposal to two recent works of mine. See Frosio (n 7) <https://goo.gl/HNkHZV>; Frosio (2017a) (n 8).

155 See Commission, Proposal for a Council Directive 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 final.

156 ibid art 6 and 28.

157 See Proposal for a Directive of the European Parliament and 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 final (25 May 2016) art 6.

158 So far, the Committee on the Internal Market and Consumer Protection (IMCO) approved an opinion on the proposed reform. See Committee on the Internal Market and Consumer Protection (IMCO), Opinion for the Committee on Legal Affairs on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market, 16 June 2017, PE 599.682v02-00, IMCO_AD(2017)599682. Also, the Culture and Education Committee (CULT) has a draft opinion in place to be voted on. See Culture and Education Committee (CULT), Draft opinion on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market, 6 February 2017, PE 595.591v01-00, CULT_PA(2017)595591. Finally, the Committee on Legal Affairs (JURI) also released

F. Fundamental Rights Implications

36 As stated by multiple authorities,[159] general filtering and monitoring obligations would be inconsistent with the Charter of Fundamental Rights of the European Union.[160] As an overall point, in *Google v. Vuitton*, the Advocate General of the CJEU pointed at the fact that general rules of civil liability (based on negligence)—rather than strict liability IP law rules—suit best the governance of the activities of Internet intermediaries:

> *[l]iability rules are more appropriate, [. . .] Instead of being able to prevent, through trade mark protection, any possible use – including, as has been observed, many lawful and even desirable uses – trade mark proprietors would have to point to specific instances giving rise to Google's liability in the context of illegal damage to their trademarks.*[161]

37 According to this argument, a negligence-based system would serve users fundamental rights. As Van Eecke mentioned, "the notice-and-take-down procedure is one of the essential mechanisms through which the eCommerce Directive achieves a balance between the interests of rightholders, online intermediaries and users."[162] Although imperfect as it is, a notice-and-take-down mechanism embeds a fundamental safeguard for freedom of information as long as it forces intermediaries to actually consider the infringing nature of the materials before coming to a final decision whether to take them down. Replacing knowledge or notice-and-take-down with filtering and monitoring obligations would by default bring about chilling effects.

38 In *Netlog* and *Scarlet Extended*, the CJEU explained that filtering measures and monitoring obligations would fail to strike a 'fair balance' between copyright and other fundamental rights.[163] In particular, they would undermine users' freedom of expression.[164] Users' freedom to receive and impart information would be struck by the proposal. Automatic infringement assessment systems might undermine the enjoyment of users' exceptions and limitations.[165] DRM effects on exceptions and limitations have been highlighted by copious literature.[166] Similar conclusions apply to this scenario. Automated systems cannot replace human judgment that should flag a certain use as fair—or falling within the scope of an exception or limitation. Also, complexities regarding the public domain status of certain works might escape the discerning capacity of content recognition technologies. At the present level of technological sophistication, false positives might cause relevant chilling effects and negatively impact users' fundamental right to freedom of expression. In the own words of the European Court of Justice, these measures:

> *could potentially undermine freedom of information, since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends*

a draft opinion and will vote on its amendments later this year. See Committee on Legal Affairs (JURI), Draft opinion on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market, 10 March 2017, PE 601.094v01-00, JURI_PR(2017)601094.

159 See C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV* (2012) ECLI:EU:C:2012:85. See also Christina Angelopoulos, 'On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market' (2017) 38-40 <https://juliareda.eu/wp-content/uploads/2017/03/angelopoulos_platforms_copyright_study.pdf>; Christina Angelopoulos, 'Sketching the Outline of a Ghost: the Fair Balance between Copyright and Fundamental Rights in Intermediary Third Party Liability' (2015) 17 Emerald Insight 72 (noting that fair balance is the appropriate conflict resolution mechanism in case of fundamental rights clashes and balancing excludes the imposition of filtering obligations on intermediaries for the purpose of copyright enforcement, but allows blocking); Stefan Kulk and Frederik J. Zuiderveen Borgesius, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2012) 34 EIPR 791, 791-794; Darren Meale, '(Case Comment) SABAM v Scarlet: Of Course Blanket Filtering of the Internet is Unlawful, But This Isn't the End of the Story' (2012) 37 Europ Intell Prop Rev 429, 432; Evangelia Psychogiopoulou, '(Case Comment) Copyright Enforcement, Human Rights Protection and the Responsibilities of Internet Service Providers After Scarlet' (2012) 38 EIPR 552, 555.

160 See Charter of Fundamental Rights of the European Union, C326/391 (26 October 2012) [hereinafter EU Charter].

161 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, joined cases, § 123 (CJEU, 23 March 2010) (Advocate General Opinion).

162 Van Eecke (n 52) 1479-1480.

163 See Netlog (n 5) § 55.

164 See Charter of Fundamental Rights of the European Union, C326/391 (26 October 2012) art 8 and 11.

165 See Leron Solomon, 'Fair Users or Content Abusers? The Automatic Flagging of Non-Infringing Videos by Content ID on Youtube' (2015) 44 Hofstra L Rev 237; Corinne Hui Yun Tan, 'Lawrence Lessig v Liberation Music Pty Ltd - YouTube's Hand (or Bots) in the Over-zealous Enforcement of Copyright' 36(6) (2014) EIPR 347, 347-351; Justyna Zygmunt, To Teach a Machine a Sense of art – Problems with Automated Methods of Fighting Copyright Infringements on the Example of YouTube Content ID, Machine Ethics and Machine Law E-Proceedings, Jagiellonin University, Cracow, Poland, November 18-19, 2016, pp. 55-56; Zoe Carpou, 'Robots, Pirates, and the Rise of the Automated Takedown Regime: Using the DMCA to Fight Piracy and Protect End-Users' (2016) 39 Colum J L & Arts 551, 564-582.

166 See Giancarlo F. Frosio, *COMMUNIA Final Report on the Digital Public Domain* (report prepared for the European Commission on behalf of the COMMUNIA Network and the NEXA Center) (2011), 99-103, 135-141 <http://www.communia-project.eu/final-report> (discussing most of the relevant literature and major threats that technological protection measures pose for fair dealings, privileged and fair uses).

on the application of statutory exceptions to copyright which vary from one Member State to another. In addition, in some Member States certain works fall within the public domain or may be posted online free of charge by the authors concerned.[167]

39 Similar points have been highlighted by miscellaneous scholarship. Enforcing online behaviour through automated or algorithmic filtering and fair use does end up inherently in a poor trade-off for fundamental and users' rights. Julie Cohen and Dan Burk argued that fair use cannot be programmed into an algorithm, so that institutional infrastructures will always be required instead.[168] Although changes in technology move fast and unpredictably, since fair use is at heart an equitable doctrine, the assumption that, judgment is not programmable might still remain valid for some time. Indeed, the capacity of neural networks to develop more accurate models of many phenomena—maybe even some or most fair uses—might change these assumptions in the future. In general, it was noted that "the design of copyright enforcement robots encodes a series of policy choices made by platforms and rightsholders and, as a result, subjects online speech and cultural participation to a new layer of private ordering and private control."[169] According to Matthew Sag, automatic copyright filtering systems—upon which private agreements between rightholders and online platforms are predicated—"not only return platforms to their gatekeeping role, but encode that role in algorithms and software."[170] In turn, automatic filtering supersedes the safe harbour system and fair use only nominally applies online.[171] In practice, private agreements and automatic filtering determine online behaviour far more "than whether that conduct is, or is not, substantively in compliance with copyright law."[172]

40 Residual critiques point at the negative externalities on innovation that this new regime would have. The ECJ emphasized the economic impact on ISPs regarding filtering and monitoring obligations. The ECJ assumed that monitoring all the electronic communications made through the network, without any limitation in time, directed to all future infringements of existing and yet to create works "would result in a serious infringement of the freedom of the hosting service provider to conduct its business."[173] Hosting providers' freedom of business would be disproportionally affected since an obligation to adopt filtering technologies would require the ISP to install a complicated, costly and permanent system at its own expense.[174] In addition, according to the ECJ, this obligation would be contrary to Article 3 of the Enforcement Directive, providing that "procedures and remedies necessary to ensure the enforcement of the intellectual property rights [. . .] shall not be unnecessarily complicated or costly [and] shall be applied in such a manner as to avoid the creation of barriers to legitimate trade."[175] UPC Telekabel also raised the issue—but less clearly—of cost of enforcement in the context of access providers. It noted that imposing costs on the access provider would limit their freedom to conduct a business, in particular by requiring to "take measures which may represent a significant cost for him, have a considerable impact on the organisation of his activities or require difficult and complex technical solutions,"[176] even though he is not the perpetrator of the infringement which has led to the adoption of that injunction.[177] Finally, however, UPC Telekabel came down with a mixed response by suggesting that access providers "can choose to put in place measures which are best adapted to the resources and abilities available,"[178] although they should "not be required to make unbearable sacrifices."[179] Notably, the Paris Court of Appeal in *Allostreaming*—which was mentioned earlier—disregarded these arguments, while imposing costs of blocking and delisting on online intermediaries alone. Similarly, *Dafra* and *Mosley* denied Google "technical impossibility" defense and claims against proactive monitoring based on cost efficiency arguments.

41 Finally, apparently, the unqualified deployment of filtering and monitoring obligations will impinge also on the service user's right to protection of personal data. In the SABAM cases, the ECJ has authoritatively already outlined the inappropriateness of these measures against fundamental rights also in this scenario. As the ECJ concluded:

requiring installation of the contested filtering system would involve the identification, systematic analysis and processing

167 Netlog (n 5) § 50.

168 See Dan Burk and Julie Cohen, 'Fair Use Infrastructure for Copyright Management Systems' (2000) Georgetown Public Law Research Paper 239731/2000 <https://ssrn.com/abstract=239731>.

169 See Matthew Sag, 'Internet Safe Harbors and the Transformation of Copyright Law' (2017) 93 Notre Dame L Rev, at 1.

170 ibid 1.

171 ibid.

172 ibid.

173 Netlog (n 5) § 46.

174 ibid.

175 See Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, 2004 O.J. (L 195) 16 (Corrigendum) Art. 3.

176 C-314/12 *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH et al* (2014) ECLI:EU:C:2014:192 § 50.

177 ibid § 53.

178 ibid § 52.

179 ibid § 53.

> *of information connected with the profiles created on the social network by its users. The information connected with those profiles is protected personal data because, in principle, it allows those users to be identified.*[180]

42 Supposedly, secrecy of communication or the right to respect for private life[181] could be also impinged upon by filtering technologies, according to the European Court of Human Rights, which tends to be critical of systems to intercept communications, especially when they monitor content of communications.[182]

G. Conclusions

43 This paper has been investigating the death of "no monitoring obligations," a well-marked trend in intermediary liability policy. In search of the culprit, this investigation has taken us all over the world to courts engaged in landmark fights with "untamable monsters." This paper explored upcoming law reform, which seeks to dismantle a twenty year old negligence-based intermediary liability system to protect the "value gap." Evidence-based analysis has also led to private ordering enforcing proactive monitoring and filtering. The death of no monitoring obligation—or at least the great danger that it's facing—finds explanation in all these factors' synergic actions.

44 Proactive monitoring obligations and filtering challenge the "fair balance" between fundamental rights in intermediary liability; either horizontal or vertical,[183] there are plenty of options to be pursued. Still, turning to proactive and automated filtering—and rejecting knowledge-and-take-down—seems hardly capable of achieving the desired "fair balance." Current Internet policy—especially in Europe—is silently drifting away from a fundamental safeguard for users' fundamental rights online, which has been guarding against any "invisible handshake" between rightholders, online intermediaries, and governments. The *Delfi* dissenting opinion reminds us that "in putting pressure and imposing liability on those who control the technological infrastructure (ISPs, etc.), [governments] create an environment in which collateral or private-party censorship is the inevitable result."[184] Professor Jack Balkin labels this process moving towards intermediaries' private ordering as "collateral censorship," which "occurs when the state holds one private party A liable for the speech of another private party B, and A has the power to block, censor, or otherwise control access to B's speech."[185] This liability, in turn, gives A "strong incentives to over-censor."[186] Historically, imposing liability on intermediaries served the censorship machine of the established power. Printing privileges—born as an innovation policy and a trade regulation—grew into a censorial tool. In this sense, online intermediary liability regulation might be following a similar path. Of course, the reason to impose liability would be always compelling enough. Today, it's the "untamable monster" of networked digital distribution and the "value gap." Yesterday, the English *Stationers' Charter* ordered that no one could exercise the art of printing but the ninety-seven "beloved and faithful" Stationers because the King and Queen manifestly perceived that:

> *certain seditious and heretical books rhymes and treaties are daily published and printed by divers scandalous malicious schismatical and heretical persons, not only moving our subjects and lieges to sedition and disobedience against us, our crown and dignity, but also to renew and move very great and detestable heresies against the faith and sound catholic doctrine of Holy Mother Church.*[187]

45 The death of "no-monitoring obligations" fits within a broader move towards enlisting online intermediaries as the Internet police. This is also achieved through the promotion of private ordering and voluntary enforcement schemes, which is a strategy prominently endorsed as part of the EU Digital Single Market Strategy. As I argue elsewhere, the intermediary liability discourse is shifting towards an intermediary responsibility discourse.[188] This process might be pushing an amorphous notion of responsibility that incentivizes intermediaries' self-intervention. Finally, intermediary responsibility does morph into algorithmic responsibility. The emergence of proactive monitoring obligations—and the automated or algorithmic enforcement they bring about—would be a conspicuous move in that direction. Looking for the answer to the machine in the machine might help taming the "monster" that Justice Salomão evoked, but at what price? Due process and fundamental guarantees

180 Netlog (n 5) § § 49.

181 See Charter (n 164) Art. 7.

182 See Kulk and Frederik J. Zuiderveen Borgesius, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2012) 34 EIPR 791, 793-794.

183 Christina Angelopoulos and Stijn Smet, 'Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability' (2016) (8(2) Journal of Media Law 266, 266 (arguing that "automatic takedown and notice-and-stay-down are applicable exclusively to child pornography.").

184 See Delfi AS (n 13) Joint Dissenting Opinion of Judges Sajò and TsoTsoria, § I.2.

185 Jack M. Balkin, 'Old-School/New-School Speech Regulation' (2014) 127 Harvard Law Review 2296, 2309.

186 See Delfi AS (n 13) Joint Dissenting Opinion of Judges Sajò and Tsotsoria § I.2.

187 *See* Stationers' Charter (1557) *in* I *A Transcript of the Registers of the Company of Stationers of London 1557-1640* (E. Arber, 1875-94) xxviii, xxx-xxxi.

188 See Frosio (n 8).

get mauled by algorithmic enforcement, trampling over fair uses, the public domain, right of critique, and silencing speech according to the mainstream ethical discourse. The upcoming reform—and the broader move that it portends—might finally slay "no monitoring obligations" and fundamental rights, rather than the untameable monster. Ultimately, the current and proposed enforcement strategies are assuming to slay the untameable monster with potions and enchantments, rather than empirical evidence.

The Role of the Principle of Effective Judicial Protection in Relation to Website Blocking Injunctions

by **Saulius Lukas Kalėda***

Abstract: The use of internet blocking to prevent access to illegal content requires the adoption of rigorous procedural safeguards. The necessity of such safeguards is even more pressing when this primarily public tool is transposed into the domain of private enforcement, for the purposes of supressing copyright and trademark infringements. Injunctions in the sphere of IP rights are governed by a net of interrelated EU legal provisions, contained in the Infosoc and the Enforcement directives (2001/29 and 2004/48), the E-Commerce directive (2000/31), and the EU net neutrality (open internet) rules (Regulation 2015/221). However, the core requirements stem from the application of the principle of proportionality and the search for a balance between competing fundamental rights. According to case law of the EU Court of Justice, the limitations upon injunctions in relation to IP rights are deduced in the process of balancing the substantive fundamental rights enshrined in the EU Charter: on the one hand, the right to the protection of intellectual property (Article 17(2)); and on the other, the freedom of expression and information (Article 11), the freedom to conduct business (Article 16), and the rights to privacy and to data protection (Articles 7 and 8). However, in relation to new types of injunctions potentially affecting the rights of multiple third parties, such as blocking injunctions, more weight should be given to procedural fundamental rights stemming from Article 47 of the Charter. This new perspective presents several advantages. Limitations resulting from Article 47 of the Charter constitute a stronger imperative than those deduced from the application of the principle of proportionality. To a large extent, they must be applied by the court of its own motion. In contrast to the principle of proportionality, fair trial requirements form part of European and national public policy provisions, potentially limiting mutual recognition of judicial decisions imposing injunctions. In the absence of harmonisation, the application of Article 47 of the Charter could therefore lead to the establishment of a minimum procedural standard, which can be invoked in order to achieve a certain degree of uniformity. This would be particularly important if blocking injunctions were to be used on an EU-wide basis.

Keywords: Copyright enforcement; injunctions; online intermediaries; judicial protection; website blocking

Recommended citation: Saulius Lukas Kalėda, The Role of the Principle of Effective Judicial Protection in Relation to Website Blocking Injunctions, 8 (2017) JIPITEC 216 para 1.

A. Introduction

1 The difficulties of enforcing IP rights in the online environment encourage the search for new tools. This consideration is reflected by the recent adoption of website blocking injunctions in the context of copyright and trade mark enforcement.[1] The growing importance of this new tool stands in

* PhD (Jagiellonian University, Kraków), Legal Secretary at the Court of Justice of the European Union (Chambers of Advocate General M. Szpunar). The views expressed are the author's own.

1 The year 2015 was dubbed 'the year of blocking injunctions' by Prof. E. Rosati on IPKat and in her editorial to Journal of Intellectual Property Law & Practice (see <http://ipkitten.blogspot.lu/2014/12/2015-year-of-blocking-injunctions.html>).

contrast to the absence of harmonised EU regulatory framework. This lacuna is partly compensated by the case law of the Court of Justice of the European Union (CJEU – or 'the Court') interpreting the requirement of striking a fair balance between fundamental rights. The application of injunctions in general, and blocking injunctions in particular, has therefore become an important terrain for the application of the EU Charter of the Fundamental Rights.

2 The Court's established case law applying the Charter to injunctions concentrates on the requirement to balance substantive fundamental rights: on the one hand, the right to the protection of intellectual property (Article 17(2) of the Charter); on the other, the freedom of expression and information (Article 11), the freedom to conduct business (Article 16), as well as the fundamental rights to privacy and to data protection (Articles 7 and 8).[2] This case law and the related national judicial practice have motivated a profound doctrinal debate. Several authors discuss the precise content of the limitations upon injunctions, which can be deduced from the proportionality test and the need to respect the rights of internet users.[3] This debate largely leaves out the underlying procedural rights.

3 Procedural safeguards stemming from the right to effective judicial protection and the right to a fair trial guaranteed by Article 47 of the Charter are necessary preconditions for the protection of substantive rights. They also constitute the conditions of legality for any judicial procedure, including the procedure for injunctive relief. In the absence of an explicit legislative framework, Article 47 constitutes the source of procedural requirements, which can ensure the right to a fair trial in the context of injunctive relief.[4]

B. Application of blocking injunctions to copyright and trade mark infringements

4 The need for appropriate procedural safeguards is particularly explicit in relation to blocking injunctions.

5 Website blocking has not yet been globally accepted as being an effective and appropriate IP enforcement tool.[5] In Europe, Germany and the Netherlands have traditionally been the least receptive to blocking for the purpose of copyright enforcement, although this attitude is changing.[6] Most countries in Europe have legislation which permits the courts to issue injunctions against third parties in the context of IP infringements. This legislation can usually be invoked in order to obtain blocking injunctions against internet service providers, although the scope of such measures varies widely.[7] In UPC Telekabel Wien,[8] the Court has clarified that website blocking lies within the scope of enforcement instruments available under EU copyright law.

6 Blocking injunctions raise more controversies than other IP enforcement tools. First, in contrast to 'notice and takedown' procedures, they are not a part of the established statutory safe harbours applicable to online intermediaries.[9] Secondly, they are not concerned with the removal of illegal content, but instead with suppressing public access to information on the internet. The technical tools used are similar to those employed by the governments for the purposes of internet censorship. This explains the political discourse, which favours "deleting"

2 See judgments in Promusicae (C-275/06, EU:C:2008:54), Scarlet Extended (C-70/10, EU:C:2011:771), SABAM (C-360/10, EU:C:2012:85), UPC Telekabel Wien (C-314/12, EU:C:2014:192), Mc Fadden (C-484/14, EU:C:2016:689).

3 See M. Husovec, Injunctions against innocent third parties: the case of website blocking, JIPITEC 4 (2012) p. 116; P. Savola, Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers, JIPITEC 5 (2014) p. 116; A. Marshoof, The blocking injunction – a critical review of its implementation in the UK in the context of the EU, IIC 46 (2015) p. 632; Ch. Geiger, E. Izyumenko, The Role of Human Rights in Copyright Enforcement Online: Elaborating a Legal Framework for Website Blocking, SSRN Electronic Journal at Researchgate (January, 2016); M. Schaefer, ISP liability for blocking access to third-party infringing content, EIPR 38 (2016) p. 633; J. Riordan, The Liability of Internet Intermediaries, Oxford OUP 2016, Chapters 14 and 15 at p. 461 et seq. Savola concludes that procedural requirements and national modalities, among others, relating to the procedural situation in court and different conceptions of preliminary injunctions, can be examined in the context of proportionality evaluation or under local procedural rules depending on their characteristics, while observing that in-depth discussion is not possible. Savola: Internet Connectivity Providers as Involuntary Copyright Enforcers: Blocking Websites in Particular (2015), text related to fns 67.

4 See with regard to the right to a fair trial in relation to internet disconnection injunctions, M. Husovec, M. Peguera, Much Ado about Little – Privately Litigated Internet Disconnection Injunctions, IIC 46 (2015) p. 27, and with regard to blocking injunctions in the field of trademark protection, A. Marshoof, The blocking injunction, *op. cit.*, p. 632.

5 For instance, concerns based on the grounds of the freedom of speech, security and effectiveness of blocking measures have so far prevented their wider adoption in the US. See "Green Paper on Copyright Policy, Creativity, and Innovation in the Digital Economy" (2013), <https://www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf>.

6 The blocking injunction was recently authorised by the German BGH, see BGH I ZR 174/14 – Goldesel.

7 See J. Riordan, The Liability of Internet Intermediaries, *op. cit.*, p. 504.

8 C-314/12, EU:C:2014:192, interpreting Article 8(3) of the Infosoc Directive (2001/29).

9 See Article 14 of the E-Commerce Directive (2000/31).

the infringing website over the "blocking" of that website.[10] A degree of internet censorship is justified in modern democratic society.[11] However, until quite recently, website blocking was considered as a tool which could be directed at public order targets, in particular, to fight child pornography and, even in this case, subject to specific safeguards.[12] Its extension to private law targets, such as copyright and trademark infringements, is a qualitatively new dimension.[13] The use of blocking for the purpose of private enforcement amplifies the need for procedural safeguards.

C. The role of Article 47 of the Charter in relation to injunctive relief

7 While conditions for granting injunctions in relation to IP rights are a matter of national law,[14] EU law contains several limitations upon injunctions. Given the lack of explicit provisions, such as those envisaged in ePrivacy Directive (2002/58), the Court has established those limitations by interpreting the fundamental rights.[15] Thus, the overarching principles derived from the Charter constitute a "maximal admissible ceiling" for the application of national rules.[16] The Court's approach to resolving conflicts of IP with other fundamental rights has drawn some criticism, as appearing to some extent motivated by pro-IP harmonisation bias.[17]

8 In imposing limitations upon injunctions, the Court has so far relied on the balancing between substantive fundamental rights, and has not yet examined the applicability of procedural rights stemming from Article 47 of the Charter. This may partly be explained by the fact that the issue of procedural rights has not been explicitly put before the Court in this context. One should also keep in mind that the conceptual analysis related to the application of Article 47 is different from the one involved in balancing substantive fundamental rights.[18] Article 47 of the Charter is not one of the competing principles involved in the balancing. Rather, the requirement of effective judicial protection underlies the whole process and serves as a "transmission belt" facilitating the effective enforcement of substantive rights. Those requirements cut both ways, ensuring effective enforcement but also protecting those who seek to defend themselves against it.[19]

9 Even though the Court has not yet referred to Article 47 in the context of IP injunctions, there is no doubt that Article 47 of the Charter is applicable to injunctive proceedings.[20] It is also true that Article 47 of the Charter has often been considered in relation to the person seeking to enforce its rights, the potential applicant in the judicial proceedings. However, Article 47 constitutes an overarching provision in relation to all aspects of fair trial, which lays down procedural guarantees applicable not only to the applicant, but also to the defendant,[21] potential co-defendants,[22] and potential third parties whose substantive rights might be affected by the procedure.[23]

10 Insofar as the safeguards relating to injunctions concern the injunctive procedure itself, they can be analysed from the perspective of Article 47 requirements. This perspective presents several advantages. Limitations resulting from Article 47 of the Charter have stronger imperative value than those deduced from the test of proportionality. To

10 As the debate in Germany, in 2010, in relation to sites containing child pornography (eg <http://www.dw.com/en/bundestag-looks-to-delete-child-pornography-websites/a-15575254>).

11 The right to freedom of expression and information (Article 10 ECHR and Article 11 of the Charter) does not prohibit prior restraints on publication. See ECtHR, Yıldırım v. Turkey (3111/10, para 47). See also Y. Akdeniz, To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression [in] New Technologies and Human Rights (Collected Courses of the Academy of European Law), Ashgate 2013, p. 56.

12 See Article 25(2) and recital 47 of Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography (OJ 2011, L 335, 261).

13 See, for a critical view on the appropriateness of blocking injunctions in the context of trade mark infringements, C. O'Doherty, Online trade mark and copyright infringement injunctions, CTLR (2016) 22, p. 79.

14 See recital 59 in the preamble to Directive 2001/29 and recital 23 in Directive 2004/48.

15 See judgments in Promusicae (C-275/06, EU:C:2008:54, paras 61-68), Scarlet Extended (C-70/10, EU:C:2011:771, paras 42-46) and UPC Telekabel Wien (C-314/12, EU:C:2014:192, para 46).

16 See in relation to internet disconnection injunctions, M. Husovec, M. Peguera, Much ado about little, *op. cit.*, p. 17.

17 See M. Husovec, Intellectual Property Rights and Integration by Conflict: The Past, Present and Future, CYELS 18 (2016), p. 239.

18 See S. Prechal, The Court of Justice and Effective Judicial Protection: What Has the Charter Changed? [in] Fundamental Rights in International and European Law, Springer 2015, p. 153.

19 See M. Safjan, D. Düsterhaus, A Union of Effective Judicial Protection: Addressing a Multi-level Challenge through the Lens of Article 47 CFREU, Yearbook of European Law 33 (2014) p. 3.

20 See, with regard to asset freezing injunction, judgment in Meroni (C-559/14, EU:C:2016:349).

21 See judgment of 11 September 2014 in A (C-112/13, EU:C:2014:2195, para 51 and the case-law cited).

22 In terms of procedural safeguards, the right to a fair trial under Article 47 of the Charter essentially means that the defendants (and co-defendants) must have the opportunity to effectively challenge the application. See opinion of AG Bobek in Dockevičius (C-587/15, EU:C:2017:234, point 111).

23 See, for instance, judgment in Meroni (C-559/14, EU:C:2016:349).

a large extent, they must be applied by the court of its own motion. In contrast to a proportionality test, which must be applied in casu, Article 47 requirements can lead to the establishment of a uniform procedural standard. While observance of proportionality pertains to the substance of the case, and cannot constitute an obstacle to mutual recognition, Article 47 requirements form part of public order provisions potentially limiting mutual recognition of judicial decisions imposing injunctions. This could be particularly important if blocking injunctions were to be used more widely and on a pan-European basis; for instance, in relation to the infringements of EU trademark.

11 The standards derived from Article 47 and those deduced while balancing substantive rights are to a large extent complementary. Some conditions, for instance, the effectiveness of an injunction, can only be assessed under the proportionality test. Some other guarantees, such as the right to apply for a review of a measure, can be deduced from both standards – since it can be viewed as affecting both the procedural position of third parties and their substantive rights. However, insofar as procedural safeguards are concerned, Article 47 constitutes a more natural and stronger framework of reference.

D. Limitations upon injunctions derived from Article 47 of the Charter

12 The right to effective judicial protection is not absolute. Numerous procedural provisions, such as time limits or application fees, can be regarded as limitations of that right.[24] Similar considerations come into play with regard to injunctive relief.[25] In this regard, the judicial procedure leading to the adoption of website blocking injunctions has several particularities. First, the adoption of a blocking injunction cannot be agreed between the parties and requires the involvement of the court. Secondly, the defendants – typically large ISPs – are neither directly nor indirectly liable for the copyright infringement. The application is made against them merely because they are in a position to enforce the injunction. In most situations the ISPs may not have an interest in opposing the order. In this respect the procedure is not in reality *inter partes*. Secondly, the blocking injunction affects at least two categories of third parties – internet users and internet services providers – who cannot intervene in the proceedings, at least, not initially. Due to those special features, the procedure leading to the blocking injunctions requires specific safeguards, which can be divided into three categories concerning: (i) the role of the court; (ii) the position of the defendant ISPs; and (iii) the position of the affected third parties.

13 All those aspects potentially connect to various elements within the bundle of rights guaranteed under Article 47 of the Charter. The principle of effective judicial protection comprises various elements; in particular, the rights of the defence, the principle of equality of arms, the right of access to a tribunal, and the right to be advised, defended and represented.[26] It is applicable in disputes between individuals and public bodies, as well as the horizontal disputes between individuals.[27] This principle encompasses appropriate, and in principle full, standard of judicial review[28] and may require the court to raise certain legal issues on its own motion.[29] The fair trial rights under Article 47 guarantee an individual's right to "effective participation" in the proceedings, which also implies that each party must be afforded a reasonable opportunity to present its case.[30] They also protect the procedural position of the defendant and, potentially, of the affected third parties.[31] The procedural safeguards stemming from the right to a fair hearing largely depend on the nature of the case. However, Article 47 of the Charter, in the same way as Article 6(1) of the ECHR,[32] imposes a certain minimum standard of fairness – in essence, the right to proper participation in the proceedings – which may be breached if a party to the proceedings, either the plaintiff or the defendant, is put in a position of procedural inequality or is not afforded adequate opportunity to present their case.

I. The role of the court

14 Balancing is inherent in the exercise of judicial function. In doubtful cases, judges must strike a balance between competing interconnected legal

24 See, for instance, judgment in Fastweb (C-19/13, EU:C:2014:2194, paras 57–58).

25 See, for instance, with regard to asset freezing injunction, judgment in Meroni (C-559/14, EU:C:2016:349).

26 See judgment in Otis and Others, C-199/11, EU:C:2012:684, paragraph 48.

27 See H. Hofmann, Article 47 – Right to an Effective Remedy [in] S. Peers, T. Hervey, J. Kenner, A. Ward, The EU Charter of Fundamental Rights. A Commentary, Hart 2014, at 47.72.

28 See judgments in Kadi II (C-584/10 P, C-593/10 P and C-595/10 P, EU:C:2013:518, paras 97-100) and KME and Others/Commission (C-272/09 P, EU:C:2011:810, paras 102-103).

29 See H. Hofmann, Article 47, *op. cit.*, at 47.77.

30 See D. Sayers, Article 47 – Right to an Effective Remedy [in] S. Peers, T. Hervey, J. Kenner, A. Ward, The EU Charter , *op. cit.*, at 47.203-47.206.

31 See fn 23 supra.

32 See O. Settem, Applications of the 'Fair Hearing' Norm in ECHR Article 6(1) to Civil Proceedings, Springer 2015, p. 89.

interests. Balancing of interests is also an explicit statutory requirement in relation to injunctive relief. In contrast to the application of clear-cut rules, balancing implies wide discretion in weighing the competing factors and, thus, requires the involvement of an independent and impartial body. In the area of fundamental rights, this task should in principle be reserved for a judicial body. The adoption of injunctions, insofar as it requires to strike a fair balance between the fundamental rights, is therefore primarily a task for the courts.[33] Additional argument for mandatory judicial involvement in the adoption of internet related injunctions could be deduced from the EU net neutrality legislation designed to safeguard open internet access. Under the Net Neutrality (Open Internet) Regulation, blocking of specific content by ISPs is prohibited subject to the exhaustive list of exceptions, which include measures necessary to comply with "orders by courts or public authorities vested with relevant powers".[34]

15 Similar considerations determine the relevant standard of judicial review. When deciding on an injunction, the court cannot accept the application even if it appears to have been agreed upon between the parties, but must carry out its own independent assessment in order to ensure an equilibrium between the competing fundamental rights. Moreover, the judicial order should be sufficiently specific in describing the measures ensuing from this balancing exercise, in order to ensure that the established equilibrium will not be compromised at the stage of the implementation.[35]

16 It may be asked whether those requirements could also be satisfied if injunctions were adopted by an independent administrative body or would result from out-of-court settlement, subject to ex-post judicial review. Concerning the first alternative, although blocking could be ordered by an administrative body in the context of public enforcement, the same does not seem appropriate in the context of private enforcement, which involves determination of rights in a dispute between private parties. As regards to the second alternative, the availability of ex-post judicial review could run counter to the principle that the balance between the competing rights must be determined at the time of the adoption of the injunction. Otherwise, the issue of fundamental rights would only be examined at the stage of implementation of the injunction.[36]

17 It may therefore be argued that Article 47 of the Charter entails the requirement that blocking injunctions must be adopted by a judicial body. As a consequence, ISPs can neither voluntarily implement a blocking measure, nor agree to it in an out-of-court settlement. The same considerations should in principle apply to the extension of blocking measures.[37]

II. The position of defendant ISPs

1. ISPs as nominal defendants

18 In the context of blocking injunctions, the defendant ISPs are in a very unusual procedural position. They are "innocent intermediaries"[38] charged with the task of implementing the injunction. Their liability is not invoked and, at all events, they are shielded by the safe harbour applicable to mere conduit intermediaries under Article 12 of the E-Commerce Directive. Their connection to the legal dispute between the rightholder and the infringer is therefore not a matter of substance, but merely a matter of legal technique. The anomalous 'nominal defendant' position of the ISPs potentially leads to a procedural disadvantage, and might have to be readjusted in order to ensure the principle of equality of arms.

19 Equality of arms is a crucial element in the concept of a fair trial enshrined in Article 47 of the Charter. This principle requires that each party to the procedure is afforded a reasonable opportunity to present its case under conditions that do not place it at a substantial disadvantage vis-à-vis the opponent. The aim of equality of arms is to ensure a balanced position between the parties to proceedings[39] (reflecting the French legal concept of "équilibre des droits des parties").[40] A procedural arrangement which puts

33 See opinions of AG Cruz Villalón in UPC Telekabel Wien (C-314/12, EU:C:2013:781, points 87 to 90) and of AG Szpunar in Mc Fadden (C-484/14, EU:C:2016:170, point 119).

34 See Article 3(3) and recital 11 of Regulation 2015/2120.

35 See opinion of AG Szpunar in Mc Fadden (C-484/14, EU:C:2016:170, point 119). Injunction formulated in general terms could be appropriate in some situations, see judgment in UPC Telekabel Wien (C-314/12, EU:C:2014:192, paragraph 52).

36 See opinion of AG Cruz Villalón in UPC Telekabel Wien (C-314/12, EU:C:2013:781, point 88).

37 The orders in Cartier incorporate a "sunset clause" such that the orders will cease to have effect at the end of a defined period "unless the ISPs consent to the orders being continued", see Cartier v BSkyB [2014] EWHC 3354 (Ch) [265].

38 The term borrowed from P. Husovec – see M. Husovec, Injunctions against innocent third parties: the case of website blocking, JIPITEC 4 (2012), p.116.

39 See judgments in Otis and Others (C-199/11, EU:C:2012:684, paras 71-72) and Sánchez Morcillo and Abril García (C-169/14, EU:C:2014:2099, para 49). The wording is borrowed from the Strasbourg case law, see ECtHR, De Haes and Gijsels v Belgium (19983/92).

40 See J.-P. Dintilhac, L'égalité des armes dans les enceinte judiciaires, Cour de cassation, Rapport 37 (2003).

one party – either applicant or defendant – at a substantial disadvantage constitutes a limitation to the rights guaranteed by Article 47 of the Charter. This consideration is relevant with regard to several aspects of blocking injunctions.

2. Liability for over-blocking

20 The first such tricky aspect concerns the lack of legal certainty with regard to the liability for over-blocking. Article 12 of the E-Commerce Directive limits the general liability of the ISPs, but only in relation to the infringements committed through the information transmitted in a network. The ISPs are not protected from the liability for over-blocking. Should the implementation of an injunction lead to over-blocking, the ISPs may be held liable with regard to Internet users. This lack of protection potentially undermines their neutral procedural position in the injunctive proceedings. Instead of accepting the order or adopting a neutral stance, the ISPs might be forced to oppose it on the grounds of their uncertain liability towards third parties. This might put the defendant ISPs in a disadvantageous position, since they would be required to oppose the order, without necessarily having access to the relevant information concerning the material infringement.

21 In his opinion in UPS Telekabel Wien, AG Cruz Villalón described similar concerns as the "ISP's dilemma".[41] He observed that if, in the interest of its customers' freedom of information, the ISP decides on a mild blocking measure, it must fear a coercive penalty. If it decides on a more severe blocking measure, it must fear a dispute with its customers. Since the ISP has no connection with the infringer and has itself not infringed the copyright – in other words, has no material connection to the dispute – the measure which forces it into such a dubious procedural situation cannot be said to strike a fair balance between the rights of the parties. In order to eliminate the ISP's dilemma, the injunctive order should define precisely what measures they are required to implement.

22 The same procedural disadvantage can be considered from the perspective of the principle of equality of arms, which entails a requirement that each party be given the possibility to present its case in the conditions that will not put it in a substantial disadvantage. In the context of application of Article 47 of the Charter to the administrative proceedings, the Court has held that in a situation where the defendant bears a procedural burden of proving a circumstance, and does not have access to relevant evidence, the court is required to use all procedures available, such as measures of inquiry, in order to safeguard the effective protection of its rights.[42] In the context of blocking injunctions, it may be argued that Article 47 of the Charter requires that the court take active measures in order to address the issue of liability for over-blocking. In particular, the court should define precisely the measures that have to be implemented by the ISP, in order to preserve their neutral procedural position in the proceedings.

3. Costs of litigation

23 The second aspect specific to the position of the ISPs relates to the repartition of costs in the injunctive proceedings.

24 The bundle of rights under Article 47 of the Charter includes a guarantee against excessively onerous costs for the participants of the judicial proceedings.[43] According to the case law of the Court of Justice – inspired by the long standing case law of the Strasbourg court – the requirement to pay court fees in civil proceedings is not in itself regarded as an incompatible restriction on the right of access to a court, but the amount of the court fees constitutes a material factor in determining whether or not a person enjoyed her right of access to a court.[44]

25 This guarantee primarily concerns financial restrictions on the access to a court, and therefore applies to the fees of application. However, it also reflects a wider principle, according to which individuals should not be prevented from seeking judicial protection merely by reason of the resulting financial burden. This principle comes into play, for instance, where a national court is called upon to make an order for costs against an unsuccessful party. The requirement that judicial proceedings should not be prohibitively expensive means that the persons should not be prevented from defending their rights before the court by reason of the financial burden that might arise as a result. This might include the capping of the costs for which the unsuccessful party may be liable.[45]

41 See opinion of AG Cruz Villalón in UPC Telekabel Wien (C-314/12, EU:C:2013:781, point 89).

42 The Court actually refers to the principle of effectiveness which is the corollary of Article 47. See judgment in Unitrading (C-437/13, EU:C:2014:2318, para 28).

43 See judgments in Orizzonte Salute (C-61/14, EU:C:2015:655, paras 72-79) and Toma (C-205/15, EU:C:2016:499, para 44).

44 See, for instance, ECtHR, Stankov v. Bulgaria (68490/01, para 52).

45 See, in the context of access to justice in environmental matters, judgment in Edwards (C-260/11, EU:C:2013:221, para 35).

26 Although these principles have been developed in relation to claimant's rights, there is no reason why they should not apply to the other party, defending its rights in the injunctive proceedings. This observation may apply to the ISPs facing the blocking injunction, since they are drawn into the proceedings due to a mere legal technicality and do not have any material interest in opposing the application. It may be argued that due to their position as nominal defendants, the ISPs should not bear the costs of proceedings. Since Article 47 of the Charter extends to pre-litigation procedures,[46] this observation also applies to any pre-litigation costs. In other words, if defendants are required to bear costs automatically, simply because of the exercise of the right to make submissions to the court, their right to a fair trial guaranteed by Article 47 might be compromised.

27 This touches upon a contentious issue. In the literature, it was observed that it would be disproportionate to require the ISPs to bear the applicant's costs.[47] However, in McFadden, the Court clarified that "taken in isolation" safe harbour under Article 12 of E-Commerce Directive does not shield the ISPs from the costs ordered in the injunctive proceedings.[48] It might be asked whether that guarantee would be different if Article 12 is applied in conjunction with the right to a fair trial. The repartition of costs in the context of blocking injunctions has also been considered by the UK courts. It appears now settled that the defendant ISPs – due to their unusual procedural position – do not have to bear the costs of an unopposed application.[49] This is however subject to the condition that the ISPs have consented to the order or at least have adopted a neutral stance. That reservation seems questionable, since it appears to penalise the defendants for pursuing their rights. Moreover, if the ISPs regularly decide not to oppose the application merely due the risk of costs liability, this might distort the application of the principle of proportionality. An undisputed application is more likely to be considered by the court as prima facie proportionate.[50]

46 See judgment in Alassini (C-317/08 to C-320/08, EU:C:2010:146, paras 55 and 57).

47 See Savola, Proportionality of Website Blocking, *op. cit.*, p. 127; and G. Spindler, Sperrverfügungen gegen Access-Provider – Klarheit aus Karlsruhe?, GRUR 2016, p. 459.

48 See para 78 of the judgment in McFadden (C-484/14, EU:C:2016:689).

49 See Cartier [2014] EWHC 3354 (Ch) [240].

50 See J. Riordan, The Liability of Internet Intermediaries, *op. cit.*, at 14.116.

III. The position of third parties

1. The fair trial guarantees for third parties

28 The guarantees stemming from the rights of the defence under Article 47 of the Charter, encompass the position of third persons whose rights may be affected by the judicial order. In several cases related to the mutual recognition of judicial decisions, the Court has clarified that the order adopted without a prior hearing of a third person whose rights may be affected is not manifestly contrary to the right to a fair trial guaranteed by Article 47 of the Charter, insofar as that third person is entitled to assert his rights before the court at a later stage.

29 In Gambazzi, in the context of a series of judicial decisions adopted without the defendant being present, the Court considered what legal remedies were available to the defendant in order to request the amendment or revocation of the provisionally adopted measures; namely, whether he had the opportunity to raise all the factual and legal issues, whether those issues were examined as to the merits in full accordance with the adversarial principle, and whether he could avail himself of procedural guarantees which gave him a genuine possibility of challenging the finally adopted measure.[51] In Meroni, the Court examined whether an asset freezing injunction issued without a prior hearing of all third persons whose rights may be affected ought to be regarded as manifestly contrary to the right to a fair trial in the light of Article 47 of the Charter. the Court observed that the contested order had no legal effect on a third person until he has received notice of it and that it was for the applicants seeking to enforce the order to ensure that the third persons concerned were duly notified of the order. Furthermore, once a third person not party to the proceedings has been notified of the order, he was entitled to challenge that order and request that it be varied or set aside.[52]

30 The principles established by the Court in relation to the fair trial rights of third affected parties are relevant to the discussion on the procedural safeguards in injunctive proceedings. The blocking injunctions affect a number of third parties who are not represented in the proceedings. This category comprises both internet users (customers of the defendant ISPs) and services providers – the operators of affected websites, including any websites that may be collaterally affected (for instance, those sharing the same IP address as the targeted site). The same also applies to the alleged infringers who, in relation to injunctive proceedings,

51 See judgment in Gambazzi (C-394/07, EU:C:2009:219, paras 41-44).

52 See judgment in Meroni (C-559/14, EU:C:2016:349, para 49).

are in a similar position as third parties.

31 It is also relevant that the breach of procedural safeguards stemming from Article 47 of the Charter may constitute the manifest breach of an essential rule of law in the EU legal order, and therefore grounds for refusal of recognition of judicial decision in another Member State on the grounds of the public policy clause.[53] In order to be effective, the Internet related injunctions in the context of the IP enforcement, might have to be applied on an EU-wide basis. This would be even more important if such injunctions were used in relation to an EU trademark. Such wider application can only be achieved – from the point of view of public order – if procedural standards stemming from Article 47 of the Charter are clearly defined and applied in a uniform manner in the EU.

32 From the point of view of the guarantees inherent in Article 47 of the Charter, the court must ensure that the affected parties are informed of the order and can effectively assert their rights by asking the court to vary or set aside the measure. In other words, those safeguards should ensure transparency and efficient ex-post review.

2. Transparency

33 Since the affected third parties may not be aware of the application for injunctions, it is essential that they receive a notice with appropriate information individually or, at least, through a general publication. This notice should enable them to ascertain the reason for the blocking (instead of returning error message), identify the applicant who obtained the order, and also inform them of the review procedure.[54] The relevant safeguards have been examined by Justice Arnold in Cartier, who held that the Internet page containing the information should not merely state that access to the website has been blocked by court order, but also identify the party or parties which obtained the order and indicate that the affected users have the right to ask the court to discharge or vary the order.[55] The requirement of transparency in this context informs third parties about the existence of restriction which is, quite evidently, a pre-condition for the exercise of the substantive fundamental rights by the affected internet users and services providers. It is therefore closely related to the existence of an effective review mechanism.

34 This requirement has already been incorporated in the blocking orders related to public enforcement[56] and is also reflected in the Council of Europe's recommendations on the use of internet filters.[57]

3. Effective review mechanism

35 The internet users and services providers whose rights are affected should have access to effective judicial remedy enabling them to challenge the blocking measure. This guarantee stems directly from the right to a court under Article 47 of the Charter, and is also closely linked to the general guarantees protecting the freedom of expression and the right to information.[58] It has already been introduced in the context of public blocking orders.[59]

36 An argument was raised in the literature that affected third parties should be given an opportunity to state their views, even before the decision is made.[60] This does not seem practically feasible – although in Cartier, Justice Arnold observed that, in theory, it would have been open to subscribers to the ISPs to apply to intervene in the case.[61]

37 In relation to the ex-post review mechanism, in UPC Telekabel Wien, the Court of Justice held that the national procedural rules must provide a possibility for internet users to assert their rights before the court, even ex-post, once the implementing measures are taken.[62] A similar requirement to ensure the existence of an effective ex-post review mechanism against traffic management measures

53 See, in relation to Article 34(1) of Regulation No 44/2001, judgments in Diageo Brands (C-681/13, EU:C:2015:471, para 50) and Meroni (C-559/14, EU:C:2016:349, para 46).

54 See, for instance, J. Riordan, The Liability of Internet Intermediaries, *op. cit.*, at 13.219-13.223 and 14.127.

55 See Cartier v BSkyB [2014] EWHC 3354 (Ch) [264] and FAPL v BT [2017] EWHC 480 Ch. [53].

56 In the context of measures combatting child pornography, pursuant to Article 25(2) of Directive 2011/93 "[website blocking] measures must be set by transparent procedures and provide 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".

57 Council of Europe's recommendation CM/Rec(2008)6, Guideline I states ; "when confronted with filters, users must be informed that a filter is active and, where appropriate, be able to identify and to control the level of filtering the content they access is subject to".

58 See ECtHR, Yıldırım v. Turkey (3111/10, para 37).

59 Pursuant to Article 25(2) of Directive 2011/93, the mandatory safeguards in the context of blocking measures must include the "possibility of judicial redress". According to Recommendation CM/Rec(2008)6, Guideline I, "[Internet users] should have the possibility to challenge the blocking or filtering of content and to seek clarifications and remedies".

60 See A. Marshoof, The blocking injunction, *op. cit.*, p. 645.

61 See Cartier v BSkyB [2014] EWHC 3354 (Ch) [263].

62 Judgment in UPC Telekabel Wien (C-314/12, EU:C:2014:192, para 57).

adopted by ISPs is reflected in the EU net neutrality rules.[63] In Cartier, Justice Arnold considered whether the injunctive order incorporates safeguards against abuse. First, those safeguards permitted the ISPs to apply to the court to discharge or vary the orders in the event of any material change of circumstances, including in respect of the costs, consequences for the parties, and effectiveness of the blocking measures. Secondly, they permitted the operators of the target websites to apply to the court to discharge or vary the orders. Thirdly, since it was debatable whether affected users could apply to discharge or vary the order under English procedural law, Justice Arnold held that orders should expressly permit affected subscribers to apply for such a remedy.[64] In FAPL, the order required a notice to be sent to each targeted hosting provider when one of its IP addresses was subject to blocking, and the operators were given permission to apply to set aside or vary the order, in the same way as the affected internet users and the operators of the target servers.[65]

38 It is debatable to what extent those EU legal provisions require an introduction of new national remedies. In Goldesel, the German BGH observed that the existing remedies are sufficient, since internet users can assert their rights against access providers on the basis of their contract with the ISP.[66] However, it is highly disputable whether such contractual, private law remedy would be sufficient in order to ensure effective review. Such a remedy is clearly insufficient with regard to collaterally affected website operators, who do not have contractual relations with the ISP[67].

39 Moreover, the adoption of new remedies might be necessary with regard to new, unorthodox types of injunctive orders, such as "live blocking orders". The review mechanism must ensure an effective and timely review. In view of this requirement, the injunctive order might have to envisage a special review mechanism with regard to the live blocking orders, which are directed at the websites that stream live content to consumers. Such orders may be adopted for a very limited period of time coinciding with the duration of the live event[68] and, therefore, any review arrangement must be extremely expedient.

4. Right to privacy and data protection

40 It is arguable whether the blocking of content available on the Internet requires to take into account the right to privacy of internet users. Thus, the BGH ruled, contrary to the opinion of the appellate court, that communications addressed to the general public do not fall within the sphere of privacy and, furthermore, the mere prevention of communication over the internet does not interfere with the right to privacy.[69]

41 Regardless of this wider debate, it seems evident that the implementation of an injunction may necessitate the adoption of adequate safeguards in relation to the right to the protection of personal data. Under the EU net neutrality rules (Article 3(4) of Regulation 2015/2120), any traffic management measure may entail processing of personal data only if such processing is necessary and proportionate to achieve the objectives set out in the permissible limitations (and, of course, must be carried out in accordance with the legislation on data protection). In the case of blocking measures, processing of personal data must be limited to what is necessary in order to comply with the court order.

42 The adequate safeguards are necessary to ensure that the knowledge obtained by the ISPs with regard to the circumstances of (blocked) communication does not interfere with internet users' right to privacy. Such knowledge must be obtained in an automated way, limited to what is necessary to block communication, recorded anonymously, using purely technical means, and deleted without a trace immediately after blocking a user's access.[70] Additional safeguards might be necessary if an injunction involves an update procedure and entails a regularly adapted list of target websites.

43 It may observed that any measures limiting the right to data protection must be provided by legislation, which should lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards against the risk of abuse.[71] It is debatable to what extent those requirements could be satisfied by a mechanism defined by a court's injunction. This aspect relates however to substantive fundamental

63 According to recital 13 of Regulation 2015/2120, any measures liable to restrict fundamental rights must be subject to adequate procedural safeguards, including effective judicial protection and due process.

64 See Cartier v BSkyB [2014] EWHC 3354 (Ch) [262]-[265].

65 See FAPL v BT [2017] EWHC 480 Ch. [27].

66 See BGH I ZR 174/14 – Goldesel [57].

67 See criticism of the approach adopted by the BGH to third party procedural rights, G. Spindler, Sperrverfügungen gegen Access-Provider, *op. cit.*, p. 457.

68 See FAPL v BT [2017] EWHC 480 Ch. The order came into force on 18 March 2017 and only endured until 22 May 2017, which was the end of the 2016/2017 Premier League season.

69 See BGH I ZR 174/14 – Goldesel [60]-[70]; and M. Schaefer, ISP liability for blocking access, *op. cit.*, p. 635.

70 See BGH I ZR 174/14 – Goldesel [68]; and M. Schaefer, ISP liability for blocking access, *op. cit.*, p. 635.

71 See judgment in Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238, paras 53-54).

rights issues and is beyond the framework of the present analysis.

E. Conclusion

44 Website blocking is an invasive enforcement tool, which requires the adoption of rigorous procedural safeguards, particularly when it is used in the context of private enforcement. The conditions for injunctions have not been harmonised in EU law and remain subject to autonomous application of national law. They must nevertheless comply with the fundamental rights guaranteed by the EU Charter. The existing case law of the EU Court of Justice and the national courts puts the emphasis on substantive limitations on injunctions, stemming from the requirement to strike a fair balance between the fundamental rights of the rightholders and internet users. The particular nature of blocking injunctions justifies putting a stronger emphasis on procedural, rather than substantive safeguards. Procedural safeguards stemming from Article 47 of the Charter could constitute a minimum standard, which could be invoked in order to achieve a certain degree of uniformity across Member States. Since breach of Article 47 of the Charter constitutes a ground for refusal of recognition of judicial decision in another Member State, such a shift of approach – from substantive to procedural rights – might be particularly important if the rightholders sought to enforce internet related injunctions on an EU-wide basis.

The Power of Positive Thinking

Intermediary Liability and the Effective Enjoyment of the Right to Freedom of Expression

by **Aleksandra Kuczerawy***

Abstract: The Internet intermediary liability regime of Directive 2000/31/EC places hosting providers in the role of private gatekeepers. By providing an incentive in the form of a liability exemption, the EU legislature has ensured that hosting providers cooperate in the policing of online content. The current mechanism results in a situation where private entities are co-opted by the State to make decisions affecting the fundamental right to freedom of expression. According to the theory of positive obligations, States not only have to refrain from interfering with fundamental human rights, but also actively protect them, including in relations between private individuals. This paper analyses whether the doctrines of positive obligations (under the European Convention on Human Rights) and effective protection (under the Charter of Fundamental Rights of the European Union) may require the States to take additional measures to protect the right to freedom of expression from interference online. In particular, the paper analyses whether the Charter may require the EU legislature to take additional measures to ensure that the right to freedom of expression can be effectively enjoyed online, for example by introducing procedural safeguards in the legal framework regarding removal of online content.

Keywords: Intermediary liability; right to freedom of expression; theory of positive obligations; fundamental rights; EU legislation; removal of online content; ECHR; CJEU

Recommended citation: Aleksandra Kuczerawy, The Power of Positive Thinking: Intermediary Liability and the Effective Enjoyment of the Right to Freedom of Expression, 8 (2017) JIPITEC 226 para 1.

A. Introduction

1 Article 14 of the E-commerce Directive (2000/31) contains a conditional liability exemption for hosting providers.[1] Under this provision, hosting service providers can benefit from a liability exemption provided they: 1) do not have actual knowledge of illegal activity or information and, as regards claims for damages, are not aware of facts or circumstances from which the illegal activity or information is apparent; 2) upon obtaining such knowledge or awareness, they act expeditiously to remove or to disable access to the information.[2]

2 The provider of a hosting service can obtain knowledge about the illegal character of hosted content in a number of ways. For example, the provider could find such content through his own activities or he could be notified about the situation

* Senior researcher and PhD candidate at the Centre for IT and IP Law (CiTiP) at KU Leuven, Belgium.

1 Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive), OJ L 178, 17.07.2000, 1.

2 Article 14.1 of the E-Commerce Directive 2000/31/EC.

by a third party. Notifications could stem either from public authorities – i.e. courts – or from private entities. In the latter case, the provider of the hosting service is called upon directly by a private individual to remove or block access to the content in question. The mechanism is commonly referred to as 'notice-and-take-down'. It is the provider's task to assess whether such a complaint is credible and make a decision about the infringing character of the content.

3 The E-Commerce Directive laid the groundwork for notice-and-take-down but did not provide any additional guidelines with regard to its implementation. Instead, the Directive left the subject matter to the discretion of the Member States.[3] Article 16 and recital (40) of the Directive encourage self-regulation in this field. Certain Member States have developed more detailed, formal notice-and-take-down procedures, but the majority of the Member States opted for a verbatim transposition of the Directive, hoping that self-regulation would emerge.[4] This however proved to be inefficient – most of the countries never introduced any self-regulatory measures.[5] The result is a lack of any firm safeguards for the content removal procedures in most of EU countries.[6]

4 As a result, the E-Commerce Directive and most national implementing laws place hosting providers in a position to decide which content can remain online and which should be removed. They may be considered as private 'gatekeepers', who are able to regulate the behaviour (and speech) of their users.[7] By providing conditional liability exemptions for third parties' illegal content or activities, the States enlist the intermediaries to enforce the public policy objectives (i.e. to remove unlawful content).[8]

5 The E-Commerce Directive is currently under review. The review process started in 2010, with a public consultation on the future of electronic commerce in the internal market.[9] Most respondents to the consultation agreed that there was no need for a revision of the E-Commerce Directive as a whole.[10] Many considered, however, that certain aspects of the Directive, particularly the intermediary liability regime, would benefit from further clarification. A more in-depth analysis of the identified issues was developed in the Commission Staff Working Document on Online Services.[11] In May 2015, the Commission announced a plan to assess the role of online platforms in the Communication on a Digital Single Market Strategy for Europe (DSM).[12]

3 Article 14.3 of the E-Commerce Directive and Recital 46 E-Commerce Directive.

4 T. Verbiest, G. Spindler *et al.*, Study on the Liability of Internet Intermediaries, Markt/2006/09/E, 12 November 2007, p. 14-16. For a more recent analysis of the national approaches to the problem of content regulation on the Internet see country reports accompanying the study by the Swiss Institute of Comparative Law, Comparative Study on Filtering, blocking and take-down of illegal content on the Internet – comparative considerations, Report commissioned by the Council of Europe, 20 December 2015 <http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>.

5 P. Van Eecke, M. Truyens, Legal analysis of a Single Market for the Information Society, New rules for a new age? A study commissioned by the European Commission's Information Society and Media Directorate-General, November 2009. Chapter 6: Liability of Online Intermediaries, p. 19. See also First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on the Directive on Electronic Commerce, COM(2003) 702 final, Brussels, 21.11.2003.

6 For an overview of issues related to the E-Commerce Directive see: Commission Staff Working Document, Online services, including e-commerce, in the Single Market, Brussels, 11.1.2012 SEC(2011) 1641 final, <http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf>.

7 The concept of a 'gatekeeper' refers to 'private parties who are able to disrupt misconduct by withholding their cooperation from wrongdoers'. Through the concept of vicarious liability, these gatekeepers can be incentivized to prevent misconducts by withholding their support, in the form of specific good, service or certification that is crucial for the wrongdoer to succeed. See H.R. Kraakman, Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy, Journal of Law, Economics, and Organization, Vol. 2, No. 1, 1986, pp. 53-105. See also E. Laidlaw, Internet gatekeepers, human rights and corporate social responsibilities. PhD thesis, 2012, The London School of Economics and Political Science (LSE).

8 See more on the practice of designating corporate actors to enforce rules on the Internet in N. Tusikov, Chokepoints - Global Private Regulation on the Internet, University of California Press, November 2016.

9 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), <http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm>.

10 European Commission, Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), <http://ec.europa.eu/internal_market/consultations/docs/2010/ecommerce/summary_report_en.pdf>.

11 Commission Staff Working Document Online services, including e-commerce, in the Single Market (n 6). For a more comprehensive discussion of these documents see A. Kuczerawy, Intermediary Liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative, Computer Law and Security Review 2015, vol. 31, Issue 1, 46-56.

12 European Commission, Commission Communication to the European Parliament, The Council, The Economic and Social Committee and The Committee of Regions, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, Brussels, 25.5.2016 COM(2016) 288 final <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0288&from=EN>.

After another consultation,[13] the Commission concluded that it would maintain the existing intermediary liability regime while implementing a sectorial, problem-driven approach.[14] This means that the Commission plans to tackle the identified problems without re-opening the E-Commerce Directive.[15] As evidenced in subsequent initiatives – that is the proposed Copyright Directive and the amendment to the AVMS Directive – the plan includes involving online service providers in content regulation. In this paper I explain why the Commission's approach is problematic. By analysing the case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the EU (CJEU), I argue that the European legislature has a legal obligation to ensure effective protection of the right to freedom of expression in the context of online content regulation. This obligation could be met by introducing procedural safeguards for freedom of expression into notice-and-take-down mechanisms. By providing the analysis, I hope to contribute to the ongoing discussion about the review of the E-Commerce Directive.

B. State interference by proxy

6 Under Article 14 of the Directive, the decision to remove or disable access to content has to be expeditious in order to exonerate the service provider from the potential liability. The most cautionary approach is to act upon any indication of illegality, without engaging in any (possibly burdensome and lengthy) balancing of rights that may come into conflict. As a result, any investigation of the illicit character of the content and balancing of rights at stake is usually non-existent.[16] This often leads to 'over-compliance' with takedown requests, or in other words, preventive over-blocking of entirely legitimate content. Article 14 of the E-Commerce Directive, therefore, creates "an incentive to systematically take down material, without hearing from the party whose material is removed".[17] The current legal situation has been characterised as an "inappropriate transfer of juridical authority to the private sector".[18] Others consider it a form of private or corporate censorship[19] possibly creating a 'chilling effect' on the right to freedom of expression.[20] Service providers are placed under such fear of liability claims that they impose on themselves measures "appropriate for making them immune to any subsequent accusation but is of a kind that threatens the freedom of expression of Internet users".[21]

7 Enlisting private entities to decide about fundamental human rights is far from ideal. The approach, however, does provide certain advantages. In the context of online expression, where information spreads in a flash, the benefits of a swift reaction are clear. Infringing or illegal content which remains online for an extended period of time can cause serious harm – some of it irreparable (e.g., reputational harm). Notice-and-take-down mechanisms provide a quick relief, far quicker than the relief typically provided by the judiciary. The indirect 'responsibilization'[22] of the

13 See European Commission, Full report on the results of the public consultation on the Regulatory environment for Platforms, Online Intermediaries and the Collaborative Economy: Online Platforms Public Consultation Synopsis Report <https://ec.europa.eu/digital-single-market/en/news/full-report-results-public-consultation-regulatory-environment-platforms-online-intermediaries>.

14 European Commission, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (n 12).

15 See S. Stalla-Bourdillon, Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the e-Commerce Directive as Well..., in L. Floridi and M. Taddeo, The Responsibilities of Online Service Providers, Springer, 2016, p. 277.

16 See discussion in C. Ahlert, C. Marsden and C. Yung, "How Liberty Disappeared from Cyberspace: the Mystery Shopper Tests Internet Content Self-Regulation" ("Mystery Shopper") at <http://www.rootsecure.net/content/downloads/pdf/liberty_disappeared_from_cyberspace.pdf>.

17 R. J. Barceló and K. Koelman, Intermediary Liability In The E-Commerce Directive: So Far So Good, But It's Not Enough, Computer Law & Security Report 2000, vol. 4, p. 231.

18 European Commission, Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (n 10) p. 12.

19 R. J. Barceló, On-line intermediary liability issues: comparing EU and US legal frameworks, E.I.P.R. 2000, 111; The Organization for Security and Co-Operation in Europe and Reporters Sans Frontiers, Joint declaration on guaranteeing media freedom on the Internet, 17-18.06.2005 <http://www.osce.org/fom/15657>.

20 See for examples concerns expressed in: Council of Europe (Council of Ministers), Declaration on freedom of communications on the Internet, 28.05.2003 <http://www.coe.int/t/informationsociety/documents/Freedom%20of%20communication%20on%20the%20Internet_en.pdf>; Council of Europe, Human rights guidelines for Internet Service Providers – Developed by the Council of Europe in co-operation with the European Internet Service Providers Association (EuroISPA), July 2008, paras 16 and 24 <http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)009_en.pdf>; T. Verbiest, Spindler G., et al., Study on the liability of Internet Intermediaries (n 4), p.15; OECD, The Economic and Social Role of Internet Intermediaries, April 2010, pp. 9-14.

21 E. Montero and Q. Van Enis, Enabling freedom of expression in light of filtering measures imposed on Internet intermediaries: Squaring the circle, Computer Law & Security Review 27 (2011) 21-35, p. 34.

22 The concept of 'responsibilization' refers to a process "whereby subjects are rendered individually responsible for a task which previously would have been the duty of another – usually a state agency – or would not have

intermediaries nevertheless creates a situation where legislation provides an incentive and gives way to potentential interference with the freedom of expression of the Internet users by private entities. The legislature therefore is indirectly contributing to the interference by private individuals – a type of 'State interference by proxy'.

8 According to human rights instruments, such as the European Convention of Human Rights (ECHR)[23] and the Charter of Fundamental Rights of the EU (CFEU),[24] States should not interfere with the exercise of protected rights (unless specific requirements are met). The States, however, have an additional obligation to effectively protect fundamental human rights from interferences by other private individuals, perhaps even more so if such interference is accepted, or even encouraged by the States.

C. Positive obligations under the ECHR

I. Do the States have positive obligations to actively protect the right to freedom of expression?

9 The right to freedom of expression constrains governments' ability to interfere in the circulation of information and ideas. In this sense, it is first and foremost a 'negative' right. However, the right to freedom of expression also contains a 'positive' dimension. According to the European Court of Human Rights, "in addition to the primarily negative undertaking of a State to abstain from interference in Convention guarantees, 'there may be positive obligations inherent' in such guarantees".[25]

10 The concept of positive obligations is based on Article 1 of the Convention, which requires that the States "shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention".[26] The concept appeared in the Court's reasoning in the late 1960's, following the *Belgian Linguistic case*.[27] It is considered to be a result of "the dynamic interpretation of the Convention in the light of changing social and moral assumptions"[28] and "the general evolution and 'socialising' of the Convention rights and freedoms".[29] Since the appearance of the concept, the Court has constantly broadened this category of obligations by adding new elements. Now almost all the standard-setting provisions of the Convention have a dual aspect in terms of their requirements.[30] The Court has not provided an authoritative definition of positive obligations.[31] The concept is described as a 'requirement to take action'[32], an 'obligation to protect', or an 'obligation to implement'.[33] In practice, positive obligations require national authorities to take the necessary measures to safeguard the right in question. The protection of rights provided by States should be practical and effective and not merely theoretical.[34] Moreover, positive obligations continue to exist even if the state 'outsources' regulation, for example to alternative regulatory bodies.[35] As the Court held in *Costello-Roberts v. the UK*, "the State cannot absolve itself from responsibility by delegating its obligations to private bodies or individuals".[36]

11 The obligation to take necessary measures to protect freedom of expression is drawn from Article 10 in conjunction with Article 1. The duty to protect

been recognized as a responsibility at all". A. Wakefield, J. Fleming, SAGE Dictionary of Policing, SAGE Publications Ltd, 14.01.2009.

23 Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), CETS No. 005, 04.11.1950, Rome, <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>.

24 Charter of Fundamental Rights of the European Union (CFEU), 2000/C 364/1, 18.12.2000, <http://www.europarl.europa.eu/charter/pdf/text_en.pdf>.

25 ECtHR, *Verein gegen Tierfabriken Schweiz (VgT) v. Switzerland*, 28 June 2001, para. 45.

26 Article 1 ECHR.

27 ECtHR, *Belgian Linguistic case*, 23 July 1968. See also ECtHR, *Marckx v. Belgium*, 13 June 1979 .

28 D. Feldman, Civil Liberties and Human Rights in England and Wales, 2nd edn., Oxford, OUP, 2002, p. 55.

29 D. Voorhoof, Critical perspectives on the scope and interpretation of Article 10 of the European Convention on Human Rights (Mass media files No. 10), Strasbourg, Council of Europe Press, 1995, p. 54.

30 J.-F. Akandji-Kombe, Human rights handbooks, No. 7. Positive Obligations under the European Convention on Human Rights. A guide to the implementation of the European Convention of Human Rights, Council of Europe, 2007, p.6.

31 A.R. Mowbray, The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights, Hart Publishing, Oxford – Portland Oregon, 2004, p. 2.

32 Dissenting Opinion of Judge Martens in ECtHR, *Gul v. Switzerland* 1996-I 165.

33 J.-F. Akandji-Kombe, Human rights handbooks, No. 7. (n 30) p.5.

34 See ECtHR, *Airey v. Ireland*, 11 September 1979, para. 24.

35 D. Voorhoof, Co-regulation and European basic rights, Presentation at the Expert Conference on Media Policy "More trust in content – The potential of self- and co-regulation in digital media", Leipzig, 9-11.05.2007, as referred to by E. Lievens, *Protecting Children in the Digital Era – the Use of Alternative Regulatory Instruments*, Leiden, Martinus Nijhoff Publishers, International Studies in Human Rights, 2010, 584 p. 388, footnote 38.

36 ECtHR, *Costello-Roberts v. the United Kingdom*, 25 March 1993, para. 27; see also, ECtHR, *Van der Mussele v. Belgium*, 23 November 1983, paras. 29-30.

the right to freedom of expression involves an obligation for governments to promote this right and to provide for an environment where it can be effectively exercised without being unduly curtailed. Such protection and promotion can take different forms. For example, it may require introducing certain measures protecting journalists against unlawful violent attacks[37], or observing the obligation of States to enact domestic legislation.[38] Perhaps the most far-reaching positive obligation in relation to freedom of expression was pronounced in *Dink v. Turkey*.[39] Here the Court considered that States are required to create a favourable environment for participation in public debate for everyone and to enable the expression of ideas and opinions without fear.[40]

12 The European Court of Human Rights accepts that Article 10 ECHR can be invoked not only in vertical relations but also in horizontal relations between individuals.[41] In such cases the horizontal effect is indirect, meaning that individuals can only enforce human rights provisions against other individuals by relying on the positive obligations of the State to protect their rights.[42] Interference by private individuals is linked, therefore, to a failure of the State to prevent the interference. This could happen, for example, in situations "where a State had taken or failed to take certain measures".[43] In *Fuentes Bobo v. Spain* the Court held that "a positive obligation can rest with the authorities to protect the freedom of expression against infringements, even by private persons".[44] Similarly, in *Özgür Gündem v. Turkey* the Court stated that "[g]enuine, effective exercise of [the right to freedom of expression] does not depend merely on the State's duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals [...]."[45]

37 ECtHR, *Özgür Gündem v. Turkey*, 16 March 2000, para. 43.

38 ECtHR, *Verein gegen Tierfabriken Schweiz (VgT) v. Switzerland*, 28 June 2001, para. 45 and 48.

39 ECtHR, *Dink v. Turkey*, 14 September 2010. See C. Angelopoulos et al., Study of fundamental rights limitations for online enforcement through self-regulation, Institute for Information Law (IViR), 2016, p. 38.

40 C. Angelopoulos et al., Study of fundamental rights limitations for online enforcement through self-regulation (n 39) p. 38, referring to ECtHR, *Dink v. Turkey*, para. 137.

41 For example ECtHR, *Fuentes Bobo v. Spain*, 29 February 2000.

42 P. Van Dijk, F. Van Hoof, A. Van Rijn, L. Zwaak (eds), *Theory and practice of the European Convention on Human Rights*, Antwerpen, Intersentia, 2006, p. 29.

43 Ibid., p. 784.

44 ECtHR, *Fuentes Bobo v. Spain*, 29 February 2000. See also: P. Van Dijk, F. Van Hoof, A. Van Rijn, L. Zwaak (eds), *Theory and practice of the European Convention on Human Rights* (n 42) pp. 784-785.

45 ECtHR, *Özgür Gündem v. Turkey*, 16 March 2000, para. 43.

II. The positive obligation to protect the right to freedom of expression vs. other Convention rights

13 The positive obligation to ensure effective enjoyment of the right to freedom of expression requires States to protect freedom of expression against infringements by private individuals. In their attempts to comply with their positive obligations, States could possibly interfere with the rights of private entities, such as the right to property or the right to conduct business. In the context of content removals by the hosting service providers, the following question can be asked: does the theory of positive obligations mean that States could force private entities to allow every type of speech on their platforms, as long as it is not prohibited by law? What would such obligation mean for thematic platforms or for content that is not illegal but inappropriate for a certain audience? Fortunately the ECtHR jurisprudence provides several pointers on this matter.

14 In *Appleby and others v. the United Kingdom*, the applicants had lodged a complaint against the UK after they were prevented from setting up a stand and distributing leaflets in a privately owned shopping centre. The Court did not find that the authorities bore any direct responsibility for the restriction on the applicants' freedom of expression.[46] The question at stake, however, was whether the UK had failed in any positive obligation to protect the exercise of the applicants' right to freedom of expression from interference by others – in this case, the owners of the shopping centre.[47] The Court acknowledged a conflict between the right to freedom of expression of the applicants and the property rights of the owner of the shopping centre under Article 1 of Protocol No. 1.[48] Despite its relevance, Article 10 does not bestow any 'freedom of forum' for the exercise of the right to freedom of expression. The applicants were able to exercise their right through several alternative means; therefore, the Court did not find that the UK failed in its positive obligation to protect the applicants' freedom of expression.[49] Nevertheless, the Court pointed out that it "would not exclude that a positive obligation could arise for the State to protect the enjoyment of the Convention rights by regulating property rights".[50]

15 The question of regulating private property to protect the right to freedom of expression was

46 ECtHR, *Appleby and others v. the United Kingdom*, 6 May 2003, para. 41.

47 Ibid., para. 41.

48 Ibid., para. 43.

49 Ibid., para. 49.

50 Ibid., para. 47.

addressed again in *Khurshid Mustafa & Tarzibachi.*[51] The case concerned the termination of a tenancy agreement by a landlord because of the tenants' refusal to dismantle a satellite dish. The dish was installed to receive television programmes from the tenants' native country. The Court acknowledged that it is not its role to settle disputes of a purely private nature. Nevertheless, it cannot remain passive where a national court's interpretation of a legal act, including a private contract, "appears unreasonable, arbitrary, discriminatory or, more broadly, inconsistent with the principles underlying the Convention".[52] The Court found, in result, that the State failed in their positive obligation to protect that right to freedom of expression.[53] This means that in order to comply with the obligation to protect the right to freedom of expression, the State might be required to set certain limits for rules that private owners establish on their property.

16 Finally, in *Melnychuk v. Ukraine* the Court clearly stated that privately-owned media, including newspapers, must be free to exercise editorial discretion to decide what articles, comments and letters submitted by private individuals they publish.[54] Nevertheless, 'exceptional circumstances' may arise "in which a newspaper may legitimately be required to publish, for example, a retraction, an apology or a judgment in a defamation case".[55] This particular case concerned the right to reply, which the Court considered an important element of freedom of expression. It follows from the need to be able to contest untruthful information, but also to ensure a plurality of opinions, especially in matters of general interest such as literary and political debate.[56] Such situations, according to the Court, may create a positive obligation for the State to ensure an individual's freedom of expression in such media.

17 The Court's recognition of positive obligations in relation to Article 10 is "nascent and piecemeal, but steady".[57] Especially in *Dink*, the essential obligation for States to ensure a favourable environment for public debate "gives a new sense of coherence to a disparate set of positive obligations" identified by the Court.[58] This optimistic note is offset by the fact that the ECHR applies only to the signatories to the Convention and the E-Commerce Directive is an instrument of the European Union. Since the EU is not (yet) a signatory to the ECHR, the ultimate framework for assessing the fundamental rights obligations of EU institutions is not the ECHR but the Charter of Fundamental Rights.

D. Effective protection of the rights in the CFEU

I. Scope of the Charter

18 The rights guaranteed by the Charter, similarly as the rights guaranteed by the Convention, can be interfered with by both States (vertical interference) and by private individuals (horizontal interference). The question is whether the Charter creates a positive obligation, in the same way as the Convention, for the States, but also for the EU acting as a legislator, to protect the Charter rights and to create an environment where these rights can be effectively enjoyed.

19 First, it should be highlighted that the meaning and the scope of the rights protected by both the ECHR and CFEU, for example the right to freedom of expression, should be the same.[59] This includes the meaning given through the jurisprudence of the Court of Human Rights which explicitly recognizes the existence of positive obligations.[60] Moreover, the EU can provide greater protection to the same right, but certainly not less.[61] According to Article 51.1, rights in the Charter must be respected, principles merely observed, but both have to be 'promoted'. Article 53 of the Charter lays down a minimum common denominator for the level of

51 ECtHR, *Khurshid Mustafa & Tarzibachi v. Sweden*, 16 December 2008, para. 45.

52 Ibid., para. 33.

53 Ibid., para. 50.

54 ECtHR, *Melnychuk v. Ukraine,* Decision of inadmissibility of the European Court of Human Rights (Second Section) of 5 July 2005.

55 Ibid.

56 Ibid.

57 C. Angelopoulos et al., Study of fundamental rights limitations for online enforcement through self-regulation (n 39) p. 38. The authors consider that this statement applies not only to Article 10 but also to other 'communication rights'. 'Communication rights' are "a term of convenience that covers a cluster of rights that are indispensable for the effective exercise of communicative freedoms. These rights typically include the right to freedom of expression, freedom of assembly and association, privacy, etc. They also include the right to an effective remedy whenever the aforementioned rights have been violated, as well as various process rights that serve to guarantee procedural fairness and justice".

58 T. McGonagle, Positive obligations concerning freedom of expression: mere potential or real power? In: O. Andreotti (ed.), Journalism at risk: Threats, challenges and perspective, Council of Europe, 2015, pp. 9-37, p. 30.

59 See Article 52.3 CFEU. See also Opinion of Advocate General Kokott in case C-73/16 *Peter Puškár*, delivered on 30 March 2017, para. 122, and CJEU, *Toma und Biroul Executorului Judecătoresc Horațiu-Vasile Cruduleci*, C-205/15, 30 June 2016, para. 41.

60 J. Blackstock, The EU Charter of Fundamental Rights: scope and competence, Justice Journal, 2012, pp. 19- 31, p. 28.

61 Ibid., p. 28.

protection of the rights. This provision, according to the Explanations of the Charter, is intended "to maintain the level of protection currently afforded within their respective scope by Union law, national law and international law"[62], with a clear emphasis on the level of protection granted in the ECHR.

20 Under the CFEU, the negative obligation (to respect) is clearly articulated. The existence of the positive obligation (to protect), however, is less obvious. Wording such as 'promotion of application of the rights' and 'protection of the rights', suggests that the scope of application encompasses both the negative and positive obligations. According to Blackstock, "even the most conservative interpretation could not deter an individual bringing an action against the State for failing to prevent the violating act of a private individual (in the exercise of a positive obligation)".[63]

II. Positive obligations under the Charter?

21 The role of positive obligations under the Charter is less developed than under the ECHR. The CJEU has, however, provided some useful guidance when interpreting EU secondary law (or implementation thereof) in light of the fundamental rights. In a number of cases the CJEU specifically addressed the issue of effective protection of the Charter rights.[64]

22 The argument of effective protection was used, for example in *Promusicae.*[65] The case was one of the first where the CJEU "relied on fundamental rights as a device of moderation".[66] The CJEU found that the disclosure of personal data at issue may be justified as it may fall within the derogation for "the protection of the rights and freedoms of others".[67] The CJEU clarified, however, that if Member States were to introduce such a measure to promote the effective protection of copyright (so the right to property), they must ensure that the measure allows for a fair balance to be struck between the various fundamental rights.[68] As a result it could be said that, "Union law does not mandate such a disclosure mechanism, but conditionally permits it, if the proportionality between fundamental rights is respected".[69]

23 A similar issue was at stake in *Coty Germany*[70], which concerned a demand for identifying information from a bank following an instance of trademark infringement. The CJEU referred to its *Promusicae* reasoning but highlighted a major difference. In *Coty Germany*, the provision of the German law at issue allowed for an unlimited and unconditional refusal to disclose the information.[71] The provision therefore prevented the effective exercise of the right to property. As a result, the ruling went further than in *Promusicae.* Instituting a remedy of disclosing personal data is no longer an optional choice for the Member States, as its absence can infringe the fundamental right to an effective remedy and the fundamental right to (intellectual) property.[72] The CJEU stated that the right to obtain information aims to "ensure the effective exercise of the fundamental right to property, which includes the intellectual property right protected in Article 17(2) of the Charter".[73] The CJEU went from recognizing the need for effective protection in *Promusicae*, to requiring that effective exercise of a fundamental right is ensured in *Coty Germany*. According to Husovec, the ruling effectively recognized a positive obligation to introduce a protective remedy.[74]

24 The need to ensure that protected rights can be exercised without undue limitation is often expressed in terms of striking the fair balance between different rights in conflict. In *Coty Germany*, the CJEU noted that "a measure which results in serious infringement of a right protected by the Charter is to be regarded as not respecting the requirement that such a fair balance be struck between the fundamental rights which must be

62 Praesidium of the Convention, Explanations relating to the Charter of Fundamental Rights, (2007/C 303/02) 14 December 2007. Explanation on Article 53.

63 J. Blackstock, The EU Charter of Fundamental Rights: scope and competence (n 60) p. 22.

64 For example, the CJEU pointed out the need for effective protection of intellectual property also in *L'Oreal v. E-Bay* case. Case C-324/09 [2011] *L'Oréal and Others* I-06011, para 131 ('effective protection of intellectual property'). See also Case C-479/04 [2006] *Laserdisken* ECR I-0808, para 62, 64.

65 The ruling was issued before the Charter became binding. Today, it would be resolved under Article 51.1 of the Charter.

66 M. Husovec, Intellectual Property Rights and Integration by Conflict: The Past, Present and Future, Cambridge Yearbook of European Legal Studies, 00 (2016), pp. 1–31, p. 10.

67 As a result of a joint reading reading of Article 15(1) of the Directive 2002/58/EC and Article 13(1)(g) of the Directive 95/46/EC. See M. Husovec, Intellectual Property Rights and Integration by Conflict: The Past, Present and Future (n 66) p. 10, footnote 52.

68 CJEU, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, C-275/06, 29 January 2008, para. 68.

69 M. Husovec, Intellectual Property Rights and Integration by Conflict: The Past, Present and Future (n 66) p. 11.

70 CJEU, *Coty Germany GmbH v. Stadtsparkasse Magdeburg,* C-580/13, 16 July 2015.

71 Ibid., para. 37.

72 M. Husovec, Intellectual Property Rights and Integration by Conflict: The Past, Present and Future (n 66) p. 19.

73 CJEU, *Coty Germany GmbH v. Stadtsparkasse Magdeburg,* C-580/13, 16 July 2015, para. 29.

74 M. Husovec, Intellectual Property Rights and Integration by Conflict: The Past, Present and Future (n 66) p. 19.

reconciled".[75]

25 In *Telekabel Wien*, the CJEU added an interesting twist to the doctrine of effective protection. According to the Court, the measures which are taken by the addressee of an injunction must be sufficiently effective to ensure genuine protection of the fundamental right at issue, that is, the right to intellectual property.[76] At the same time, however, the CJEU reiterated that the right to intellectual property is not inviolable and that nothing in the wording of Article 17.2 CFEU suggests that it must be absolutely protected.[77] For this reason, when the addressee of an injunction chooses the measures to be adopted, he must ensure compliance with the fundamental right of Internet users to freedom of information.[78] Effectively, the CJEU imposed the duty to balance the fundamental rights at stake directly on intermediaries, instead of the States.[79] The CJEU continued to specify that the adopted measures must serve to bring an end to a third party's infringement of copyright or of a related right but without affecting Internet users who are using the provider's services to lawfully access information.[80] If such a result was not achieved, "the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued".[81]

III. Compatibility with the Charter

26 Both EU secondary law and national law falling within the scope of EU law must be interpreted in light of the Charter.[82] Moreover, any possible conflicts with fundamental rights can be tested against the Charter, which provides grounds for judicial review.[83] The CJEU can declare a national provision implementing EU law incompatible under Art. 51.1 CFEU.[84] Upon a request based on Art. 267 TFEU the CJEU can also directly invalidate a provision or a whole act of secondary Union law, such as a directive.[85]

27 In *Digital Rights Ireland*, the CJEU was called upon to assess the compatibility of the Data Retention Directive (2006/24/EC) with the Charter (specifically with Articles 7, 8, and 11 of the Charter).[86] First, the CJEU established that the Directive constituted an interference with the right to privacy and data protection.[87] In the following analysis the CJEU declared that that the interference was prescribed by law and that it did not adversely affect the essence of the rights to privacy and data protection.[88] The crucial point of the analysis, therefore, was the question of proportionality of the administered measures. The CJEU found that the Directive defined no limits of the scope, and failed to lay down any objective criterion to determine the limits of the access to the retained data.[89] Furthermore, the Directive did not contain sufficient substantive and procedural conditions relating to the access and reuse of the retained data. Instead, the Directive merely provided that the procedures and the conditions were to be defined by each Member State in accordance with necessity and proportionality requirements.[90] For these reasons, the CJEU decided that Directive 2006/24 did not provide for sufficient safeguards to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data.[91] The CJEU ruled that "the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter"[92] and declared the Directive invalid.[93] Arguably, the CJEU did not refer explicitly to positive obligations but pointed out the lack of effective protection, which should have been ensured by providing sufficient safeguards. It is therefore clearly an example of a legislature's failure to act. The result of the failure was a disproportionate interference which led the CJEU to declare the Directive non-compliant with the Charter and invalidating it entirely.

28 Similar arguments were used by the CJEU in 2015 to invalidate the EC Decision 2000/520/EC on the adequacy of the protection provided by the safe

75 CJEU, *Coty Germany GmbH v. Stadtsparkasse Magdeburg*, C-580/13, 16 July 2015, para. 35.

76 CJEU, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*, C-314/12, 27 March 2014, para. 62.

77 Ibid., para. 61.

78 Ibid., para. 55.

79 C. Angelopoulos, S. Smet, Notice-and-fair-balance: how to reach a compromise between fundamental rights in European intermediary liability, Journal of Media Law, 2016, 8:2, pp. 266-301, p. 281.

80 CJEU, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*, C-314/12, 27 March 2014, para. 56.

81 Ibid., para. 56.

82 K. Lenaerts, Exploring the Limits of the EU Charter of Fundamental Rights, European Constitutional Law Review, 2012, Vol.8(3), pp.375-403 , p. 376.

83 Ibid., p. 376.

84 See CJEU, *Hernández and Others*, Case C-198/13, 10 July 2014, para. 33-36.

85 Article 267 TFEU, Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390.

86 CJEU, *Digital Rights Ireland Ltd and Seitlinger and others*, Joined Cases C-293/12 and C 594/12, 8 April 2014, para. 17 – 21.

87 Ibid., para. 34 – 37.

88 Ibid., paras. 39 and 40.

89 Ibid., para. 60.

90 Ibid., para. 61.

91 Ibid., para. 66.

92 Ibid., para. 69.

93 Ibid., para. 71.

harbour privacy principles.[94] In *Schrems* the CJEU observed that Decision 2000/520/EC enabled interference, founded on national security and public interest requirements or on domestic legislation of the US, with the fundamental rights of the individuals whose personal data is transferred from the EU to the US.[95] Moreover, Decision 2000/520 did not contain any finding regarding the existence of rules adopted by the US intended to limit such interference[96] nor did it refer to the existence of effective legal protection against interference of that kind.[97] Referring to *Digital Rights Ireland*, the CJEU repeated that EU legislation involving interference with the fundamental rights (guaranteed in Articles 7 and 8 CFEU) must lay down clear and precise rules governing the scope and application of a measure and impose minimum safeguards, so that the persons concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use.[98] Likewise, the CJEU observed that legislation not providing for any possibility for an individual to pursue legal remedies to have access to his personal data, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as provided in Article 47 CFEU.[99] In light of these findings, the CJEU declared the decision invalid.[100]

29 Based on the analysis above, I would argue that there exists a positive obligation to ensure that fundamental rights under the Charter can be exercised effectively. Even without an explicit reference to the doctrine of positive obligations, the CJEU is clearly able to achieve a similar result using the principle of proportionality and the requirements of fair balancing and effective protection. Moreover, the CJEU should take into account the meaning and scope of the protection given through the jurisprudence of the European Court of Human Rights. The obligation applies not only to the Member States when they implement EU law, but also the EU acting as a legislator. It would be unreasonable to think that the EU can demand compliance with the Charter rights from the Member States when they implement EU law, but would not itself be obliged to comply. This conclusion finds support also in the CJEU's observations in *Kadi I*, stating that "all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness which it is for the Court to review".[101]

E. Private enforcement of public policy objectives

30 It is evident that EU secondary law can be invalidated for not respecting the Charter rights. In case of *Digital Rights Ireland*, the interference with the fundamental right at issue was rather direct, as the Directive required the retention of data by telecom operators. It was therefore a clear example of State interference. In case of the E-Commerce Directive, the interference with the right to freedom of expression is not direct. The liability exemptions do not require the hosting service providers to remove content. Content removal is, however, often a result of the provision in Article 14 of the E-Commerce Directive. It is a situation of a horizontal interference resulting from a failure of the legislature (EU) to effectively protect the right to freedom of expression – a form of 'State interference by proxy'.

31 This type of approach, unfortunately, is becoming a new trend at the EU level. It can be traced in numerous attempts to responsibilize online platforms for regulating content. For example, it is apparent in the Code of Conduct on Countering Illegal Hate Speech Online announced by the Commission in May 2016.[102] The initiative which was launched in cooperation with a select number of IT companies, urges these companies to 'take the lead' on countering the spread of illegal hate speech online.[103] Delegation of enforcement activities from State to private companies seems even bolder than the limited liability regime in the E-Commerce Directive. Strictly speaking, any interference with freedom

94 CJEU, *Maximillian Schrems v. Data Protection Commissioner*, C-362/14, 6 October 2015.

95 Ibid., para. 87.

96 Ibid., para. 88.

97 Ibid., para. 89.

98 Ibid., para. 91.

99 Ibid., para. 95.

100 Ibid., paras. 97, 98, 104, 105.

101 CJEU, *Yassin Abdullah Kadi and Al Barakaat International Foundation v. Council of the European Union and Commission of the European Communities (Kadi I)*, Joined cases C-402/05 P and C-415/05 P, 3 September 2008, para. 285. See also *Schmidberger*, where the CJEU stated that "measures which are incompatible with observance of the human rights thus recognised are not acceptable in the Community", CJEU, *Eugen Schmidberger, Internationale Transporte und Planzüge v. Republik Österreich*, C-112/00, 12 June 2003, para. 73.

102 The Code of Conduct on Countering Illegal Hate Speech Online, <http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf>.

103 For more criticism of the Code by civil society organisations see: EDRi, Guide to the Code of Conduct on Hate Speech, 3 June 2016, <https://edri.org/guide-code-conduct-hate-speech/>; Article 19, EU: European Commission's Code of conduct for Countering Illegal Hate Speech Online and the Framework Decision – legal analysis, June 2016, <https://www.article19.org/data/files/medialibrary/38430/EU-Code-of-conduct-analysis-FINAL.pdf>; A. Kuczerawy, The Code of Conduct on Online Hate Speech: an example of state interference by proxy? 20 July 2016, <https://www.law.kuleuven.be/citip/blog/the-code-of-conduct-on-online-hate-speech-an-example-of-state-interference-by-proxy/>.

of expression resulting from the implementation of the Code cannot be attributed directly to the Commission (as the restrictions will be administered by the IT companies 'voluntarily'[104]). Nevertheless, it is clear that the Commission's role is more than that of a facilitator. The Commission is no longer merely incentivizing content control by intermediaries but actively requesting them to remove certain types of content. By inviting private companies to restrict speech of individuals, the Commission becomes an initiator of the interference with a fundamental right by private individuals. The role of the Commission is confirmed by the statements urging the IT companies to act faster to tackle online hate speech or face laws forcing them to do so.[105] Similar concerns can be formulated in relation to the Commission's proposals on a new directive on copyright in the Digital Single Market[106] and an amendment to the AVMS Directive.[107] The former requires the service providers to monitor their platforms for copyright-infringing content[108] while the latter requires video-sharing and possibly social media platforms to restrict access to harmful – but not necessarily illegal - content (to protect minors) and to incitement to violence or hatred (to protect all citizens)[109]. It seems that the Commission's solution to the problem of illegal and harmful online content without re-opening the E-Commerce Directive is to require private entities to take action.[110] Yet, private parties, such as intermediaries, "should be made to follow the legal rules provided by national (and supra-national) authorities, not forced to invent them".[111] None of these initiatives, however, contain clear safeguards to ensure effective protection to the right to freedom of expression.[112] Their compliance with the Charter is therefore highly questionable.

F. Safeguards for freedom of expression

32 To be justified, any interference with the right to freedom of expression must be prescribed by law, administered for a legitimate aim, and proportionate. Notice-and-take-down procedures should contain appropriate safeguards to ensure that these conditions are met. Inspiration for such safeguards could be drawn from the procedures that already exist in countries that implemented more detailed regulations.[113] Moreover, input could be found in the numerous responses provided to the public consultations organized so far by the Commission.[114] Below I present examples of safeguards that the Commission could consider. The following selection does not aim to be exhaustive but merely constitutes a preface to a more detailed discussion.

104 Such agreements cannot really be considered as truly voluntary as they often arise under governmental pressure and threats of legal action to compel private companies to adopt non-legally binding enforcement measures. See more in N. Tusikov, Chokepoints - Global Private Regulation on the Internet (n 8) p. 4.

105 See European Commission, Fighting illegal online hate speech: first assessment of the new code of conduct, 6.12.2016, <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50840>.

106 Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, Brussels, 14.9.2016, COM(2016) 593 final - 2016/0280 (COD), <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0593>.

107 Proposal for a Directive 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, Brussels, 25.5.2016 , COM/2016/0287 final - 2016/0151 (COD), <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1464618463840&uri=COM:2016:287:FIN>.

108 See more in S. Stalla-Bourdillon et al., Open Letter to the European Commission - On the Importance of Preserving the Consistency and Integrity of the EU Acquis Relating to Content Monitoring within the Information Society, 19 October 2016, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2850483>; and S. Stalla-Bourdillon et al., A Brief Exegesis of the Proposed Copyright Directive, 30 November 2016, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2875296>.

109 See more in M. Fernández Pérez, VMSD: European Parliament set to vote whether it's allowed to vote, 17 May 2017, <https://edri.org/avmsd-european-parliament-set-to-vote-whether-its-allowed-to-vote/>.

110 See European Commission, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (n 12).

111 C. Angelopoulos, S. Smet, Notice-and-fair-balance: how to reach a compromise between fundamental rights in European intermediary liability (n 79) p. 283.

112 See also M. Schaake et al., Open letter sent to Commissioner Ansip - MEPs want notice and action directive, 10 May 2107, <https://marietjeschaake.eu/en/meps-want-notice-and-action-directive>.

113 In the EU, several countries chose to use the opportunity provided by Art. 14.3 of the E-Commerce Directive to introduce more detailed measures for removal of online content. For example, such specific laws exists for example in Finland in the Finish Information Society Code, in France in the LCEN Law No. 2004-575 of 21 June 2004 on ensuring confidence in the digital economy, and in Hungary in Act CVIII of 2001 on certain issues of electronic commerce services and information society services.

114 For example, European Commission, Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (n 10); European Commission, Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries, Summary of responses, <http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet/summary-of-responses_en.pdf>; European Commission, Full report on the results of the public consultation on the Regulatory environment for Platforms, Online Intermediaries and the Collaborative Economy (n 13).

33 From a human rights perspective, content removal mechanisms should have a sufficient basis in law. To meet this requirement, the EU legislature should introduce specific legal provisions to clarify removal procedures. Notice-and-take-down procedures should clearly state whether they apply to specific types of content or activities, or whether they take a horizontal approach (as in the E-Commerce Directive).[115] Moreover, the procedure should state specifically if it distinguishes any type of 'manifestly illegal' content which the service providers should remove after obtaining knowledge of its existence, regardless of how they obtained such knowledge.[116]

34 Legislation providing for a notice-and-take-down procedure should meet the requirement of 'quality'.[117] This means it should be compatible with the rule of law, accessible and foreseeable. The latter requirement means that rules should be clear and sufficiently precise for those subject to them to foresee the consequences and adjust their behaviour accordingly.[118] For example, laws providing specific notice-and-take down procedures could clarify the measures which a host may take out on its own initiative and the measures which it may only take after a court order or order by an administrative authority.[119] The procedures might further describe whether the request must be first submitted to the content provider[120] and the following order of events, starting with the notification to the service provider.[121] Moreover, the procedures could specify the timeframes for different actions and the formal requirements for a valid notice.[122] Especially rules regulating the latter are relevant because the validity of notice often determines the existence of actual knowledge. This approach is consistent with the CJEU ruling in *L'Oreal SA v. eBay,* which stated that notification should be sufficiently precise and adequately substantiated.[123]

35 Safeguards should also introduce elements of proportionality, due process and procedural fairness into the notice-and-take-down procedures. One possible safeguard consists of requiring a notification to content providers informing them that a complaint has been filed. The role of the notification should not be limited to informing the content providers that their content is about to be removed or already has been removed (or made inaccessible), but it should allow them to respond with a defence of the use of the content (a counter-notification).[124] The notification introduces elements of a fair hearing, but also elements of equality of arms and of adversarial proceedings as it enables both parties involved to have knowledge of and comment on the evidence and the observations made by the other party. The right to due process also requires that decisions about rights and obligations should adequately state the reasons on which they are based. Even if the removal decisions are taken by private entities, it is not unreasonable to expect them to state the reasons for the interference in the notification.[125]

36 Safeguards should also ensure that everyone whose rights have been interfered with have a right to effective remedy. This means that they should have at their disposal a measure that would allow for an appropriate relief by stopping the violation, or allowing the victim to obtain adequate redress. In case of content removals from the Internet, the right to effective remedy is equally relevant for both

115 For example the procedure described in the Finnish Information Society Code applies specifically to the content infringing copyright or neighbouring rights while the procedure implemented in France does not contain such delineation and applies to any content in violation with the national law. See Chapter 22 of the Finish Information Society Code (2014/917), which entered into force on 1 January 2015, Tietoyhteiskuntakaari, 7.11.2014/917, <http://www.finlex.fi/en/laki/kaannokset/2014/en20140917.pdf> and Loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, Version consolidée au 15 mai 2017 , <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164>.

116 For example in Finland hosting providers are obliged to act based upon their knowledge when the content in question consists of hate speech, or pictures with child pornography, sexual violence or intercourse with an animal. The content must be "clearly contrary" to the Criminal Code's provisions on this type of content. See also European Commission, Full report on the results of the public consultation on the Regulatory environment for Platforms, Online Intermediaries and the Collaborative Economy (n 13) p. 17.

117 See ECtHR, *Ahmet Yıldırım v. Turkey,* 18 March 2013, para. 57.

118 See ECtHR, *Sunday Times v. the United Kingdom*, 26 April 1979, para. 49.

119 Swiss Institute of Comparative Law, Comparative Study on Filtering, blocking and take-down of illegal content on the Internet – comparative considerations (n 4) p. 798.

120 See also European Commission, Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries, Summary of responses (n 114) p. 5.

121 See for example European Commission, Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (n 10) p. 12.

122 See for example European Commission, Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries, Summary of responses (n 114) p. 3-7.

123 CJEU, *L'Oreal SA v. eBay*, Case C324/09, 12 July 2011, para. 122.

124 See more on the counter-notice procedure in European Commission, Full report on the results of the public consultation on the Regulatory environment for Platforms, Online Intermediaries and the Collaborative Economy (n 13) p. 17.

125 Such a requirement exists, for example, in Finland where the Information Society Code provides that the notification to the content provider must state the reason for removal (or blocking), Section 187 of the Finish Information Society Code.

sides of the conflict. Victims of infringing expression should have access to an effective remedy to stop the infringement, for example by requesting removal or blocking. Content providers whose content was wrongfully removed should in turn have the possibility to contest the removal and to request that the content be reinstated, for example through the counter-notification and 'put-back' procedure.[126] Moreover, there should always exist a possibility of judicial redress to ensure effective legal protection of the right to freedom of expression.[127] A possibility of reviewing the removal decisions by independent courts also provide an additional safeguard that the fundamental rights at stake are balanced fairly.

G. Conclusion

37 Under the Convention and the Charter, interference with freedom of expression may be permitted if it is prescribed by law, for a legitimate aim, and proportionate. Delegating powers to make decisions regarding fundamental human rights – such as freedom of expression – to private entities should come equipped with certain protective measures in place. The doctrine of positive obligations requires States to take action necessary to ensure effective enjoyment of fundamental rights. The idea of positive obligations in the context of Article 10 ECHR has been developing slowly but, as is evident from the Strasbourg case law, such obligations nevertheless exist. The same could be argued in the context of the Charter, even if the phenomenon is branded differently, as 'effective protection'.

38 At present the E-Commerce Directive is lacking any safeguards that could ensure such protection and fair balance regarding the right to freedom of expression. Moreover, only a handful of countries have introduced any additional safeguards in this matter. The situation resembles the problem of the Data Retention Directive, where the EU legislature failed to provide for adequate safeguards to protect the fundamental rights at stake. Therefore, I would argue that the EU is currently not complying with the positive obligation to protect the right to freedom of expression from disproportionate interference by private entities in the context of the notice-and-take down mechanisms. Of course the EU is not subject to the jurisdiction of the ECtHR so it cannot be held responsible in Strasbourg for violations by private entities. However, if an instrument of EU secondary law fails to comply with the CFEU, it can be invalidated by the CJEU, as demonstrated in *Digital Rights Ireland.* The requirement to ensure effective protection could be satisfied by implementing procedural safeguards into the legislation which provides a basis for the notice-and-take-down mechanisms. The procedural safeguards could introduce the elements of quality of law, due process and proportionality into the delegated private enforcement system. Since the E-Commerce Directive is currently undergoing a review process, this seems to be the right moment to make a call reminding the EU legislature about the obligation to comply with its own fundamental rights framework.

Acknowledgments

The research leading to this paper has received funding from the KU Leuven OT project: "Legal Norms for Online Social Networks - Case Study of Data Interoperability" and the Flemish research institute imec (formerly iMinds).

The author would like to thank Tarlach McGonagle and Martin Husovec for their guidance in my research and the anonymous reviewer for their valuable comments and feedback.

126 For example, appeal mechanisms are foreseen in Finland (Section 193 of the Finish Information Society Code) and Hungary (Article 13.7 of the Hungarian Act CVIII of 2001 on certain issues of electronic commerce services and information society services). See also European Commission, Full report on the results of the public consultation on the Regulatory environment for Platforms, Online Intermediaries and the Collaborative Economy (n 13) p. 17-18.

127 See for example Section 187 of the Finish Information Society Code.

What Does It Matter Who is Browsing?

ISP Liability and the Right to Anonymity

by **Ciarán Burke and Alexandra Molitorisová***

Abstract: Disputes concatenating privacy, speech and security through the right to anonymity are particularly hard cases to adjudicate. The traditional paradigm, according to which anonymity plays a double role – protecting fundamental rights, as well as potentially threatening them – continues to drive policies that, in turn, emphasise the risks and downplay the opportunities of anonymity in the online world. The content/metadata distinction is a residue of such ambiguous views, persistent in the Court of Justice of the European Union's (CJEU) approach towards the right to anonymity in ISP liability cases. The article initially explores the argumentative grounds behind the CJEU's recent McFadden judgment (part B). Against the backdrop of the theory of balancing of interests, this paper critically examines the Court's reductionist position. Our critique suggests a method of avoiding the disproportionately narrow scope of analysis that accompanies this position. For this purpose, we establish the right to anonymity at the periphery of both the freedom of expression and information, and the right to private life and data protection, while contesting the right to anonymity as a right sui generis. We proceed with three key points. By inspecting the nature of the right to anonymity, we unveil the interconnectedness between the right to freedom of expression and information and the right to private life and data protection (part C). Chilling effects represent an often understated evidence of this relationship. In addition, we see that affecting certain means of exercising a particular fundamental right, such as is its anonymous exercise, brings forward important extra-legal considerations, facilitating the discernment of chilling effects in any analysis of human rights. It is argued that regulating anonymity could pose a significant obstacle to the exercise of a fundamental right as a whole, and consequently impact upon the core of that right (part D). Harmonisation-driven attempts to develop human rights guarantees, framed in seemingly robust procedures established by the CJEU, at the level of data collection or retention as well as data disclosure by an ISP, have the potential to be derailed by nation-specific considerations. Taking such considerations seriously can reverse the imminent impact upon the core of the fundamental rights in question, which the narrow scope of traditional human rights analysis easily discounts. This requires diverting from the "targeting by dissuasion" argument as a mere technical exercise, and acknowledging the subtle subterranean relationship of the fundamental rights being considered (part E).

Keywords: ISP liability; right to anonymity; Mc Fadden; chilling effects; fundamental rights; privacy; CJEU

Recommended citation: Ciarán Burke and Alexandra Molitorisová, What Does It Matter Who is Browsing? ISP Liability and the Right to Anonymity, 8 (2017) JIPITEC 238 para 1.

A. Anonymity: Disguised in Crowds and Technology

1 Let us briefly look back through the lens of history:

2 Ceausescu fell from power on 21 December 1989. In the last moment of his rule, to demonstrate the regime's lasting grip over the nation, the party's apparatus held a rally counting 80,000 people in the streets of Bucharest. Romanian citizens were instructed to pause their work and tune in the parade on their radios and televisions. Ceausescu appeared on the balcony at the headquarters of the Romanian Communist Party and overlooked the crowds. He praised the success of the Romanian socialism, and promised raising social benefits. "I want to thank the initiators and organisers of this great event in Bucharest, considering it is a...", he never finished his sentence. Eight minutes after the speech commenced, a person booed in the crowd and sparked the resistance of nearby bystanders as well as thousands of people sitting at the radios and televisions in what came down in history as the Romanian revolution. Until today, that person remains unidentified.[1]

3 Between 19 and 21 October 1905, uncontrollable violence spread over the city of Odessa. In the wake of the October Manifesto, and anti-imperialist propaganda flooding Russian cities, violent clashes with the Jewish population engulfed the city. For many involved, the cause of the Russian decline preceding these turbulent events became instantaneously self-evident and needed to be eradicated. Around 400 Jewish perished in the hands of unnamed crowds in just two days. A number of police and military officers benefited from the anonymity conveyed by pogroms, and disguised in civilian clothes participated in the massacre, instead of maintaining law and order. Likely, the perpetrators of these atrocities will never be identified.

4 Although the above examples demonstrate that the question of anonymity has long been considered both crucial and contested in terms of ensuring both societal order and individual liberty, this paper aims to add a contemporary perspective to the debate concerning the frictional relationship between anonymity and the protection of fundamental rights and freedoms. Such an intervention is warranted by the seemingly novel, but perhaps quite analogous, circumstances of modern society: online anonymity, enabled by technological advancements and endorsed by billions of indistinguishable Internet users, provides for similar risks and opportunities. On the one hand, anonymity diminishes accountability: it gives "license" to depart from the limits of legality in the sense of positive law, and permits individuals to escape accountability for the possible ramifications of their actions. On the other hand, anonymity empowers individuals in terms of their autonomy and personhood,[2] and protects them from unjustified interference with certain fundamental rights. Human experience has shown on countless occasions that an additional "shield" reinforcing the freedom of expression, such as a speech act made in anonymity, can be of existential importance to its exercise. If history is characterised by a continuous narrative of civilisation, anonymity, in turn, becomes instrumental, so that marginal discourses are not excluded from the conversation. This is often the case with regard to the expression of ideas that offend, shock or disturb, and call for more protection than information and ideas that are favourably received.[3] Since the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression, enabling participation in political and societal activities and discussions, even a minor disruption within the Internet's architecture bears the risk of significant collateral damage.[4] Recalling the real-world situations of political expression of the past essentially brings the problem closer to the everyday experience of today: pervading online real-name policies attach identity more strongly (visibly and permanently) to every act of online expression than almost any real-world situation has ever done before;[5] and available technologies significantly facilitate the ways in which one's identity can be revealed,[6] such as data mining. A modern judge adjudicating hard cases at the intersection of privacy, speech, and security must thus become increasingly aware of the importance of users'

* Prof. Dr. Ciarán Burke is a Professor of International Law, Friedrich Schiller University Jena, Germany, ciaran.burke@eui.eu.

Mgr. Alexandra Molitorisová is a Research Assistant to Prof. Dr. Ciarán Burke, Friedrich Schiller University Jena, Germany, alex.molitorisova@gmail.com.

1 Harari, Y. N., Homo Deus: A Brief History of Tomorrow, Harvill Secker London, 2016, pp. 135-137.

2 Moyakine E., Online Anonymity in the Modern Digital Age: Quest for a Legal Right, Journal of Information, Rights, Policy and Practice, Vol 1, No 1 (2016), p. 4.

3 Handyside v United Kingdom, Merits, App No 5493/72, A/24, [1976] ECHR 5, (1976) 1 EHRR 737, (1979) 1 EHRR 737, IHRL 14 (ECHR 1976), 7th December 1976, ECtHR, para 49.

4 Ahmet Yildirim v Turkey, Merits, App No 3111/10, 18th December 1976, Second Section, ECtHR para 54.

5 Madrigal A., Why Facebook and Google's Concept of 'Real Names' Is Revolutionary, in The Atlantis, 5 August 2011, available at: <https://www.theatlantic.com/technology/archive/2011/08/why-facebook-and-googles-concept-of-real-names-is-revolutionary/243171/> (accessed on 10 March 2017).

6 Zingales N., Virtues and perils of anonymity: should intermediaries bear the burden?, TILEC Discussion Paper, DP 2014-025, July 2014, available at: <http://ssrn.com/abstract=2463564> (accessed on 10 March 2017).

individual preferences regarding identity disclosure when they exercise their freedom of expression.[7] At the same time, acknowledging the importance of anonymity and confidentiality on the Internet must not lead the same modern judge to refuse to protect the rights of others.[8] We will show in our account that in adjudicating the hard cases, it is especially his or her local knowledge of users, their preferences and behaviour, and possible causes of chilling effects in the local environment, that would have a particularly instructive force in the analysis.

5 The right to data protection and the right to private life benefit from anonymous exercise on similar terms. The anonymization of data provides for the ultimate protection of an individual, in the sense that anonymised data are not considered personal data as long as the data subject is not identifiable. Processing anonymized data can, in theory, never violate subject's right to privacy. Per Article 32(1)(a) of the General Data Protection Regulation (GDPR), anonymization (or pseudonymization) of personal data is considered necessary for ensuring data security when such data processing, in accordance with Article 6(1)(f) GDPR, is of legitimate interest to a controller.[9] Anonymization is further not only required under the current Directive 2002/58/EC on privacy and electronic communications as a *lex specialis* (E-Privacy Directive) with regard to traffic data (e.g. routing, duration of communication, location of terminal equipment, IP address), but is also explicitly upheld in Recital 9 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data (DPD) as a measure minimising the risks associated with data processing.

6 In order to contextualise criticism of the right to anonymity in legal terms, the dual character of anonymity must be further stressed throughout the article, as a grey zone between illegality and legality, as a tenet of protected fundamental rights, as well as a potential source of interference with other fundamental rights, which renders any kind of conflict involving a purported right to anonymity especially difficult to balance. For the purposes of understanding anonymity deontologically in online communication networks, we should consider the right to anonymity particularly with respect to two fundamental rights; namely, the right to private life and protection of personal data (Articles 7 and 8 of the Charter and Article 8 of the ECHR, with the latter conceived of solely as a right to privacy), and the right to freedom of expression and information (Article 10 ECHR, Article 19 UDHR, Article 11 of the Charter).

7 The right to anonymity was once again contemplated at the highest level of the European judiciary structure. In its recent judgment,[10] the Court of Justice of the European Union (CJEU or Court) concluded that Article 12(1) and (3) of Directive 2000/31 (the E-Commerce Directive) and Directives 2001/29 and 2004/48 did not preclude the grant of an injunction, requiring a provider of access to a communication network allowing the public to connect to the Internet to take a measure consisting in password-protecting the Internet connection, provided that users were required to reveal their identity in order to obtain a password and could not therefore act anonymously, so to prevent third parties from making a particular copyright-protected work available to the general public. In its analysis, the CJEU refrained from even briefly considering the protection of personal data. The balancing of interests test exclusively concerned the right to property versus the right to conduct business and the right to freedom of information. For the purposes of this article, the *Mc Fadden* judgment serves as a *point de départ* towards a critical assessment of the CJEU's piecemeal approach in adjudicating the right to anonymity. The critical analysis shows that framing matters. The way in which the right to anonymity is shaped, differs when considered in what we call pure data protection cases (recently, e.g. in *re Breyer* and *Tele2*), and when balanced against other rights in mixed cases, in which the frame of adjudication is dictated by these other rights (e.g. in IP and ISP liability cases, in *re Promusicae* and *Scarlet Extended*). This article does not plan to defend the right to anonymity. It rather reveals that, while being unable to outlaw anonymity as such on the one hand, and facing increasing difficulties in justifying certain indiscriminate identification measures on the other, the Court engages in soft behavioural techniques of effectively nudging (incentivising) users out of the anonymous space, so as to eliminate the risky grey zone in which anonymous Internet users operate. Marginally, it also points to a differentiation between users' content and metadata, and to the fact that while this differentiation is becoming less and less visible in data protection cases, its remnants retain a certain degree of relevance in mixed cases where the risks accompanying anonymity arise.

7 Delfi v Estonia, Merits, App No 64569/09, Chamber Judgment [2013] ECHR 941, 10th October 2013, ECtHR, para 92.

8 Ibid.

9 Esayas S. Y., The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach, in European Journal of Law and Technology, Vol 6, No 2, 2015.

10 Judgment of the Court (Third Chamber) of 15 September 2016, Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, C-484/14, ECLI:EU:C:2016:68.

B. Anonymity as Privacy in the Mc Fadden Judgment

8 The *Mc Fadden* case represents a recent example of a mixed case – a category of disputes in which the right to privacy is invoked in the context of a litigation concerning another fundamental right (here, the right to property). Specifically, Sony Music asserted that its rights were infringed when its copyright protected work was made available on the Internet to the general public by means of a Wi-Fi network owned by Mr. Mc Fadden. Mr Mc Fadden was an entrepreneur, who facilitated anonymous access to that network free of charge as part of his marketing activities. In *re Mc Fadden*, the Court avoided answering, or even indicating, what broader societal ramifications the proposed measure could provoke. However, the fact that the right to data protection and the right to private life of Internet users were absent in the balancing of interests test[11] did not pass unnoticed.[12] The injunction imposed upon an ISP consisting of the mandatory identification of all of a network's users can unquestionably eliminate users' anonymity. In that regard, AG Szpunar posited that the obligation to register users and retain their data is clearly disproportionate to the pursued goal – securing the legitimate interests of third parties – and that the means selected provoke serious reservations concerning the protection of the right to privacy and the confidentiality of communications.[13] Similar arguments are echoed by a number of commentators,[14] and the authors of this article, too, sympathise with these calls for caution. However, in order to expose the convoluted relationship of the right to privacy and the right to freedom of expression and information through the right to anonymity, we propose that we should not rush to decide that the judges' reasoning is based upon an erroneous worldview or that it represents a technical error.[15] As a starting premise, we intend to accept that, in this case, societal concerns can be given their due weight in the balancing of legitimate interests, without explicitly weighting the right to privacy. This will aid in illustrating that while facing persistent criticism of playing a "catch me if you can" game with technological advancements, regulating the online environment involves exploring interdependencies of privacy, speech and security as freedom mediators, in order to induce deliberate changes in a decision context, minimising the risk of human behaviour.[16]

9 Primarily, two legal bases could be considered in parallel to ensure that such an identification measure – as proposed by the Court – works in accordance with law: (a) consent of the data subject; and (b) compliance with obligations to which the data controller is subject. First, measures could be implemented in such a way as to ask an individual to provide consent to data processing in order to access the Internet. Such technical measures can, for instance, consist of real-name policy requirements or of verification via an e-mail address, Facebook account, ID card or telephone number. The Court implies that it is the right to *freedom of information* which is solely affected here.[17] If a data subject is not prepared to make this privacy trade-off, the right to freedom of expression and information would suffer considerably. As a general criticism, such framing appears excessively narrow, and the Court's reassurance that an open Wi-Fi connection constitutes only one of several means of accessing the Internet[18] is insufficient. In many people's perception, it would not be a stretch to say that a data subject is *coerced* into surrendering a part of his or her privacy in exchange for exercising freedom of information. However, if multiple options to access the Internet exist, this exchange remains completely voluntary, and thus, compatible with a legitimate ground for data processing (Article 7(a) DPD). Such a situation would resemble requiring prior consent for the storage of cookies (per Article 5(3) of the E-Privacy Directive), where, if not consented to, many websites, including search engines, remain inaccessible to the Internet users,[19] a practice widely tolerated by the European

11 Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 90.

12 Husovec M., Holey Cap! CJEU Drills (Yet) Another Hole in the E-Commerce Directive's Safe Harbors Holey Cap!, Forthcoming, Journal of Intellectual Property Law & Practice (JIPLP), published as draft at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843816> (accessed on 15 March 2017).

13 Opinion of Advocate General Szpunar delivered on 16 March 2016, Mc Fadden, C-484/14, ECLI:EU:C:2016:170, para 146.

14 Cholasta R., Korbel F., CJEU's judgment is opening the way for limiting anonymous access to the Internet <http://www.lexology.com/library/detail.aspx?g=dc9449ea-046b-4292-8a9f-59bccdf37a32> (accessed on 15 March 2017) or Stalla-Bourdillon S., The CJEU rules on free access to wireless local area networks in McFadden: The last(?) shudder of Article 15 ECD, the vanishing of effective remedies, and a big farewell to free Wi-Fi!, available at <https://peepbeep.wordpress.com/2016/09/15/the-cjeu-rules-on-free-access-to-wireless-local-area-networks-in-mcfadden-the-last-shrudder-of-article-15-ecd-the-vanishing-of-effective-remedies-and-a-big-farewell-to-free-wi-fi/> (accessed on 28 July 2017).

15 For criticism of balancing test, see McFadden P. M., Balancing Test, Boston College of Law Review, Vol 29:585, May 1988, p. 644.

16 See in the context of German constitutional debate, Schweizer M, Nudging and the Principle of Proportionality, in Mathis K., Tor A. (eds.), Nudging, Possibilities, Limitations and Applications in European Law, Springer (2016), p. 114.

17 Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 82 and 83.

18 Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 92.

19 For some types of cookies the consent is not mandatory. Those cookies include any technical information or information necessary for the provision of services. Under the proposed Regulation on Privacy and Electronic

regulator. The decision whether or not this practice amounts to an interference with privacy rights, remains within the sole disposition of the decision maker.[20] Moreover, the DPD itself and national data protection laws based upon its transposition already balance the fundamental rights at stake,[21] and provide for mechanisms maintaining a certain equilibrium, by setting default data protection standards and safeguards.[22] Therefore, if the human rights dimension is to be addressed with precision, it may be useful to centre the analysis around the effects of such a measure on the right to freedom of information.[23]

10 Secondly, the injunction imposes a duty to process certain personal data on the part of the ISP. The ISP may choose not to provide a space for consent with data processing to its users. Consent is only one of several legal grounds for the processing of personal data, and it does not exclude the possibility that other legal grounds may be appropriate to consider in a given case.[24] In that instance, Article 7(c) DPD prescribes that if national law enables the imposition of a specific obligation (here, for example, storing users' IP addresses and external ports), the data processing can be said to be necessary for compliance with a legal obligation to which the controller is subject. An ISP is forced by law to implement certain identification measures, which triggers the scrutiny of its legitimate interests in the balancing test, especially the freedom to conduct business. The Court holds that where a measure consists of marginal changes to the exercise of the ISP's activity, such a measure does not impact upon the essence of this freedom,[25] even if the ISP cannot choose between multiple options to terminate or prevent infringement. Yet, noticeably, in *re UPC Telekabel,*[26] if that ISP is left with more than one technical means to comply with an injunction (in addition to identification measures, the Court could, for example, consider limiting the type of communication passing through the Wi-Fi network), a domestic court must be able to exercise a secondary judicial review of a measure imposed on or implemented by the ISP. This leaves the balancing test interestingly unsettled, because the proportionality of a particular technical measure is assessed by a national court only *a posteriori* and only incidentally, with likely diverging outcomes. In our opinion, *re Mc Fadden* could be read in a similar fashion. The domestic court should ascertain whether revealing a user's identity in order to obtain a password to access a communication network would prevent the users acting anonymously and dissuade them from infringing copyright via peer-to-peer platforms.[27] At its core, given the differences in the identification measures contemplated, the national judge is supposed to assess the effectiveness (or the proportionality) of the relevant measure. The Court suggests that the eradication of users' anonymity may ensure genuine protection of the fundamental rights at issue,[28] and the national judge shall, in his or her turn, consider whether a particular identification measure is indeed capable of achieving the stated aim.[29] This includes answering the question as to whether the implemented measure goes beyond what is strictly necessary. It seems that in the case, it is possible to pursue the second step of the proportionality analysis in the proceedings before the national court, ergo re-open the aspects of privacy protection, and in particular data retention, in the legal analysis. In the final part of the article, we propose a guideline by which a national judge can consider approaching this dimension and re-join the human rights analysis in his or her part.

11 In the proportionality analysis, the question of whether the measure is strictly targeted, and does not impact upon a fundamental right more than is necessary, is only answered vis-à-vis the right to freedom of information. No other rights are considered. This has much to do with the European courts' view of the role of the Internet as a facilitator of the dissemination of information,[30] which enhances new forms of social interaction and revolutionizes the public's access to news.[31] Therefore, the measure should, above all, not affect the possibility of Internet users to lawfully access information using the provider's services,[32] a goal which should, in principle, be satisfied by

Communications no consent will be required for non-privacy intrusive cookies (e.g. the history of shopping cart).

20 Article 29 Working Party, Opinion 15/2011 on the definition of consent (WP 187), 13 July 2011.

21 Notably, Recital 37 and Article 9 of the DPD.

22 Judgment of the Court of 6 November 2003, Bodil Lindqvist, C-101/01, ECLI:EU:C:2003:596, para 82.

23 To criticism of human rights inflation in the online environment, e.g. De Hert, P., Kloza, D., Internet (access) as a new fundamental right. Inflating the current rights framework?, European Journal of Law and Technology, Vol. 3. No. 3, 2012.

24 Article 29 Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", WP 217, 9 April 2014.

25 Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 91.

26 Judgement of the Court (Fourth Chamber) of 27 March 2014, UPC Telekabel Wien, Case C-314/12, ECLI:EU:C:2014:192, para 57.

27 Judgment in Mc Fadden, ECLI:EU:C:2016:68, at 96 and 10.

28 Ibid, at 101.

29 Husovec M., supra note xii.

30 Times Newspapers Limited v the United Kingdom, App Nos 3002/03 and 23676/03, [2009] EMLR 14, 10th March 2009, ECtHR, para 27.

31 Opinion of Advocate General Jääskinen delivered on 25 June 2013, Case C-131/12, Google Spain, ECLI:EU:C:2013:424, para 121.

32 Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 93.

not terminating the connection or blocking any Internet site as a source of information.[33] The right to information carries the risk of sharing or allowing others to share proprietary material of a third party or information of personal character; therefore, it necessarily involves a risk of fundamental conflict with the right to property,[34] or the right to privacy. Such a conflict must be resolved in accordance with the idea of achieving a fair balance.[35] This requires, in essence, assessing the problem of necessity, which the Court epitomizes through the notion of a targeted measure. If a measure does not block the transmission of lawful communication (e.g. due to the implementation of a system that inadequately distinguishes between unlawful and lawful content), the requirement of a strictly targeted measure is fulfilled.[36] In view of the foregoing, the fact that the injunction does not restrict access to available online sources appears a critical point. The implementation of the identification measures can change many aspects of such service – from unprotected to protected, from secure to insecure, from anonymous to non-anonymous network – but does not block the transmission. One cannot know beforehand what a user's true preference is,[37] e.g. to log into an anonymous network. Each default situation carries the possibility of untargeted side effects,[38] excluding one group from the use of the network. There may be users who would, in principle, never log into an anonymous or public network. Therefore, reversal of the situations does not necessarily interfere with the user's freedom to choose (here, to use a particular service).[39] The injunction is supposed to fulfil a dissuasive function[40] of unlawful use of the provider's services, and the Court appears to suggest that only secure and non-anonymous networks target such illicit use, and *ergo*, are proportionate to the aim pursued. In so doing, the Court pre-arranges the ground for testing the basic proportionality (see above). The acceptance that dissuasion does not in principle interfere with the lawful user's autonomy of will could explain why the Court addressed only the right to freedom of information and the right to conduct a business. In our conclusion, we will debate how the lack of harmonisation concerning data disclosure rules and the dissuasive function, which the injunction assumes, leads the analysis to its denouement by a national court, possessing nation-specific information.

C. Privacy, Browsing and Chilling Effects

12 Outlining the arguments that we believe might underline the Court's reasoning, reveals one notable argumentative lacuna that draws us away from the reductionist position. This lacuna is found in the Court's failing to consider so-called chilling effects. The lacuna will have to be filled by the reasoning of a national judge. Chilling effects bring into the legal analysis what is, in part, an extra-legal consideration (the same way a lack of legal certainty,[41] extensive interpretation of derogations, or the severity of punishment[42] affect human behaviour), and can sometimes become more problematic from a human rights perspective than direct infringements or interferences. A deterrent effect manifests itself as a shared negative human feeling regarding the lawful exercise of a fundamental right and can amount to an unwarranted abrogation of that right, with respect to particular individuals, sensitive groups, or the general population.

13 Chilling effects only become visible if the analytical focus is detached from the direct unlawful interference[43] and the letter of law. This requires a deeper understanding of: (i) the (meta)normative dimension of the interdependence of the relevant fundamental rights; and (ii) psychological, sociological, economic, and other factors that can influence the factual exercise of a particular fundamental right. Any understanding of the interdependencies is subject to the scope of analysis – what rights a judge is prepared to consider. It is a problematic, often perilous, trait of the balancing test to rightly identify the competing interests, not only of the litigants themselves, but also the broader interests that the litigants represent[44] and those that

33 Ahmet Yıldırım v. Turkey, Cengiz, App No, ECtHR and Others v. Turkey, App No, ECtHR, and further in Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 92.

34 See e.g. Ashby Donald et Autres c France, App No 36769/08, 10 January 2013, ECtHR.

35 Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 98.

36 Judgement of the Court in UPC Telekabel Wien, ECLI:EU:C:2014:192, para 56, Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 93, and similarly, from Judgment of the Court (Third Chamber) of 24 November 2011, Scarlet Extended, ECLI:EU:C:2011:771, C-70/10 para 52.

37 Schweizer M, supra note xvi, pp. 100-101.

38 Insecure public networks leave the Internet user to deal with several inherent risks (e.g. data theft), and discourage lawful exercise of the right to information.

39 Schweizer M., supra note xvi, pp. 100-101.

40 Judgement of the Court in UPC Telekabel Wien, ECLI:EU:C:2014:192, and Judgment in Mc Fadden, ECLI:EU:C:2016:68.

41 See Cumhuriyet Vakfı and Others v Turkey, App No 28255/07, 8th October 2013, ECtHR.

42 Mosley v the United Kingdom, App No 48009/08, 10th May 2011, ECtHR or Morice v. France [GC], App No 29369/10, ECHR 2015, ECtHR ("*where fines are concerned as a moderate type of sanction, it would not suffice to negate the risk of chilling effects on the freedom of expression*", para 176).

43 In this case, affecting the possibility of using the ISP's services to access information lawfully. See Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 94.

44 McFadden P. M., supra note xv, p. 586.

they can further advocate. It does not always become explicit, which fundamental rights should be placed onto the balancing scale and weighed against each other; for instance, in *re Delfi v Estonia*, the landmark case concerning the role of the ISP in regulating anonymous speech on the Internet, the ECtHR did not deal with the ISPs' freedom to conduct business, or in *re Google Spain*, notoriously known as the "right to be forgotten" case, the CJEU did not refer to a publisher's right to freedom of expression,[45] and denied any particular weight to Google's freedom of entrepreneurship. Furthermore, as regards point (ii), the widely accepted understanding of law as a system of rules prescribing and governing human behaviour[46] reveals why such factors matter in the analytical discussion: if a person comports with one rule, however, simultaneously, his behaviour thwarts the anticipated objective pursued by a second rule, the contradiction demands a resolution. The more limited the scope of the analysis is, the more difficult it is to detect the relevant impact on the other, co-existent, legitimate objectives. Sometimes only first exploring the extra-legal considerations (societal dimensions) reveal what fundamental rights it is specifically germane to address.

14 The mutual interdependence of the right to freedom of expression and right to privacy has been recognised by a number of authorities.[47] Chilling effects constitute often-cited evidence of the existence of this relationship.[48] However, this has not been the case with regard to the right to information, to which the Court confines its ruling. By examining the content of this right, several issues come to the surface: (i) the right to information covers both the right to impart and receive information[49] (i.e. establishes a broad right to communication, both private and public); (ii) the right covers not only the information, but also the way in which the information is conveyed,[50] *ergo*, it covers all means of communication;[51] and (iii) the right to information must be understood as a pre-condition of exercising freedom of expression[52] in its narrow sense.[53] What is the connection with the right to privacy? First of all, as regards the right to data protection, it has the distinctive feature of being both technologically and contextually neutral,[54] it is applicable to personal data passing through all means of communication. Furthermore, it is clear that private communication is an inseparable component of the right to private life.[55] The extent of Article 7 of the Charter corresponds to Article 8 ECHR; however, the word "communication" replaced the word "correspondence", to cover the wide variety of means through which people nowadays communicate both privately and publically.[56] However, if Article 11 of the Charter makes an apparent distinction between "information" and "ideas", this differentiation makes it more difficult to accept that the chilling effects caused by an interference with the right to privacy could impact upon the right to information equally to the freedom of expression, conceived narrowly. If information, in contrast to ideas, bears the badge of being "impersonal", "factual", and supposedly "impartial", the fact that the exercise of the right to information can be chilled by such interference is easily discounted. However, such a description is detached from today's reality. In a world where users are stimulated to overshare their personal data[57] and where the expression of public statements and private sentiments passes through the same communication means, imparting information (even if directed to a restricted group of recipients) potentially encompasses enormous breadth. To illustrate this, let us consider a few examples. Two interpretations of a single fact may appear on social

45 Fomperosa Rivero Á., Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality, Stanford-Vienna Transatlantic Technology Law Forum, European Union Law Working Papers, No 19, p. 21.

46 Kelsen H., General Theory of Law and State, translated by Wedberg A., Harvard University Press, 1945, p. 3.

47 See Scharsach and News Verlagsgesellschaft mbH. v Austria, App No 39394/98, ECHR 2003-XI, ECtHR, para 30. Also as Frank La Rue, former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression stated in his 2013 Report to the Human Rights Council noted: "*Privacy and freedom of expression are interlinked and mutually dependent*".

48 E.g. seminal Schauer F., Fear, Risk, and the First Amendment: Unraveling the "Chilling Effect," 58 B.U. L. REV. 685, 730 (1978).

49 See Article 11(1) of the Charter.

50 See, i.a., Jersild v Denmark, App No 15890/89, 24th September 1994, ECtHR (GK), para 31; 24.2.1997, De Haes and Gijsels v Belgium, App No 19983/92, 29th March 2001, ECtHR, para 48; Thoma v Luxembourg, App No 38432/97, 12th September 2001, ECtHR para 45, Palomo Sánchez v Spain, App No 28.955/06, 28th October 2014, ECtHR, para 53.

51 Murat Vural v Turkey, App No 9540/07, 21st October 2014, ECtHR, para 52.

52 See Open Door and Dublin Well Woman v Ireland, App Nos 14234/88 u 14235/88, 29th October 1992, ECtHR.

53 Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users Explanatory Memorandum, available at: <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c6f85>, p. 40 (accessed on 8 March 2017).

54 Lynskey O., Deconstructing data protection: the "added-value" of a right to data protection in the EU legal order, 63 International & Comparative Law Quarterly (2014), p. 577.

55 Article 7 of the Charter (Respect for private and family life) prescribes that everyone has the right to respect for his or her private and family life, home and *communications*.

56 Explanations relating to the Charter of Fundamental Rights. Official Journal of the European Union C 303/17 - 14.12.2007.

57 See Jozwiak M., Balancing the Rights to Data Protection and Freedom of Expression and Information by the Court of Justice of the European Union. The Vulnerability of Rights in an Online Context, 23 MJ 3 (2016), p. 419.

media accounts in the following manner:

a) One third of stock market inventors believe that at least one country will leave the Eurozone in the next 5 years;

b) Two-thirds of stock market investors believe that all Eurozone countries will stay in the monetary union for the next 5 years.

15 An individual's reaction to share (i.e. to immediately impart information that was just accessed) one of the two interpretations of a certain piece of information can depend on how that information is framed, and the preference to share one piece of information over another can reveal much about the individual's political stance. Two Google searches[58] could look like this:

a) Basic income doomed to fail;

b) Happy people; basic income; Finland.

16 Alternatively, two browsing paths could consist of the following steps/clicks:

a) Edward Snowden – Is Edward Snowden a Hero? – Bernie Sanders on the Exile of Snowden;

b) Edward Snowden – Is Edward Snowden a Hero or Traitor? - Obama Says Snowden is Not a Patriot.

17 The frame employed by a user, or the links the user clicks, can reveal much about his own interests, constituting a significant component of privacy. An aggregation of the imparted or accessed information can generate a representative overview of the individual's political and other opinions.[59] The right to freedom of expression is not more susceptible to be affected by the chilling effects prompted by lawful interferences with privacy than the 'mere' right to information. Although more empirical data is needed as regards users' browsing behaviour, similar observations were made with respect to decreasing traffic to or avoidance of several Wikipedia articles that raised privacy concerns in the post-Snowden era, such as those containing words like "jihad", "al-Qaeda", "suicide attack", "Islamist", or "Dirty Bomb".[60] Clearly, the ability to freely access information is as intrinsically linked to privacy as holding one's opinions and expressing them. As the freedom of expression and right to information are both indispensable for "uninhibited, robust, and wide-open"[61] debate and communication,[62] understanding that chilling effects can occur with respect to each right equally is essential for future analytical purposes. In order to ensure the human rights dimension of the online environment, the right to freedom of expression and information should not be arbitrarily separated. It is perhaps only encouraging that the CJEU is not always oblivious to potential behavioural effects that an interference with the right to privacy might provoke. In *DRI*, it noted that: "the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance".[63] It remains germane to ask what primary interferences with the right to privacy may trigger these effects. In legal terms, does an entitlement to exercise a particular fundamental right anonymously exist, and if so, under what conditions may such an entitlement be abridged?

D. Anonymity on the Periphery of Fundamental Rights

18 In attempting to construct a permission to enjoy particular rights anonymously as a *right* to anonymity,[64] separable from the rights being enjoyed, one can be guided by the principle of equality before law. Fundamental rights stem from the doctrine of universality,[65] and are conferred upon *everyone* on a non-discriminatory basis, regardless of origin. Alternatively, the right to anonymity can be said to stem from the principle of personal autonomy,[66] as the ability to conduct one's life in a manner of one's choosing,[67] as well as the freedom to make decisions,

58 According to AG Jääskinen in Google Spain, ECLI:EU:C:2013:424, search processes constitute an important concretisation of the freedom of expression.

59 Ohm P., Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review 1701 (2010).

60 Penney J. W., Chilling Effects: Online Surveillance and Wikipedia Use, 31 Berkeley Tech. L.J. 117 (2016).

61 New York Times v Sullivan, 376 U.S. 967 84 S. Ct. 1130 12 L. Ed. 2d 83 1964 U.S., U.S. Supreme Court.

62 Wachter S., Privacy: Primus Inter Pares Privacy as a precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903514> (accessed on 8 March 2017).

63 Judgment of the Court of 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, C-293/12, ECLI:EU:C:2014:238, para 37.

64 Moyakine E, supra note ii.

65 Nickel, James. Making Sense of Human Rights: Philosophical Reflections on the Universal Declaration of Human Rights, (Berkeley; University of California Press, 1987), pp. 561-2.

66 *Per* AG Maduro's opinion in case C-303/06 S. Coleman v Attridge Law and Steve Law, on 31 January 2008, ECLI:EU:C:2008:61, personal autonomy and human dignity are values underlying the principle of equality, para 8.

67 Pretty v the United Kingdom, App No 2346/02, 29th April

the freedom to act (including contractual liberty),[68] the freedom to choose to be left alone,[69] or the *right* to establish details of one's identity as an individual human being.[70] It is a principle that underpins the interpretation of *all* guarantees of the ECHR.[71] However, both constructs appear challenging; first of all, the right to anonymity *per se* does not find its legal basis in the current *lex lata* – neither universality nor autonomy can be neatly reduced to anonymity. Secondly, there exists a strong dialectical relationship with a number of recognised fundamental rights (the right to assembly, freedom of religion, freedom of thought, freedom of expression and freedom of association); it stands in a position, from which it potentially overlaps with several of these rights simultaneously. Therefore, it is difficult to grant anonymity the benefit of a separate positive right *sui generis*. With this criticism in mind, it is proposed to view the right to anonymity as a right that potentially dwells within the penumbra of other rights. Several of the Court's judgments[72] as well as recent EU policy and legislative decisions and more traditional policies of the Member States endorsing real name identification requirements preclude a contrary view. These measures on the one hand, and advocating restrictive positions on the compulsory identification of users accessing the Internet or using encryption technologies on the other,[73] leave policy-makers with a complex political problem. Anonymity makes for a malleable phenomenon, the risks and benefits of which are, in turn, accentuated and depreciated vis-à-vis a particular policy objective. For example, the Commission's latest proposal to review the Anti-Money Laundering Directive avows that in the context of virtual currency markets, anonymity is rather a hindrance than an asset and calls for the identification of users of virtual exchange platforms and custodian wallet services.[74] A similar trend is indicated by the adoption of the Directive on the Passenger Name Record Data.[75] Also, traditionally, at the level of the Member States, mandatory identification measures relate to many private or public law areas such as hotel guest registration, company ownership, or real estate purchase publicity. On the other hand, concerns about de-anonymization and re-identification of data sources persist, and are considered a serious obstacle to an EU-wide data-driven economy.[76]

19 The core, as opposed to the penumbra, of a fundamental right, is generally constructed as an absolute limit to balancing.[77] It customarily refers to certain important elements[78] that together constitute the very substance of the right.[79] If the core of a fundamental right is to be preserved, the balancing test should not touch upon these elements. However, the situation with the right to data protection and right to private life is rather more entangled. One can sense a certain paradox in stating that a freedom to choose whether to be identifiable, identified or to remain in anonymity, does not constitute the core of the right to privacy, notably if one concedes that: (i) anonymization is the strongest form of data protection (anonymised data are not considered personal data); and (ii) Article 7 of the Charter centres around personal autonomy,[80] i.e.

2002, ECtHR, para 62.

68 Judgment of the Court of 5 October 1999, Kingdom of Spain v Commission of the European Communities, Case C-240/97, ECLI:EU:C:1999:479, para 99.

69 See Marshall J., Personal Freedom through Human Rights Law? Autonomy, Identity and Integrity under the European Convention on Human Rights, Martinus Nijhoff Publishers, Leiden, 2009.

70 Goodwin v the United Kingdom, App No 28957/95, 11th July 2002, ECtHR (GC), para 90.

71 Ibid.

72 E.g. Judgment of the Court of 19 October 2016, Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779 and Judgment in Mc Fadden, ECLI:EU:C:2016:68.

73 See e.g. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, available at: <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>, pp. 88 and 89 (accessed on 7 March 2017).

74 Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC (COM(2016) 450 final).

75 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

76 EPSC Strategic Notes, 11 January 2017, available at: <https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_21.pdf> (accessed on 6 March 2017).

77 von Bogdandy A., Kottman M., Antpöhler C., Dickschen J., Hentrei S., et altri, Reverse Solange – Protecting the Essence of Fundamental Rights against EU Member States, Common Market Law Review, 49.2 (Apr 2012), pp. 489 to 519.

78 On the essence of fundamental rights, see Brkan M., In search of the concept of essence of EU fundamental rights through the prism of data privacy, Maastricht Faculty of Law Working Paper 2017-01, pp. 13 to 15.

79 There are instances when the Court interpret the core of a fundamental right as a very possibility of exercising of the right ("*being carried out as such*", in Judgment of the Court of 20 May 2003 Österreichischer Rundfunk u.a., C-465/00, ECLI:EU:C:2003:294, at 49). Nonetheless, at other instances, the court avows that if the wording of the Charter does not suggest that the right is inviolable (such as in contrast the right to life), there is no reason that to absolutely protect such a right (Judgment of the Court of 16 February 2012, SABAM, C-360/10, ECLI:EU:C:2003:294, at 41). Also, similarly to Article 17 ECHR, which states that the ECHR may not "*be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein*."

80 See Commentary of the Charter of Fundamental Rights of the European Union. ECtHR too places personal autonomy

freedom *largo sensu*, including making decision about whether to remain anonymous or what information concerning an individual should be anonymised. However, these points appear mutually self-reinforcing, and if they should validate the position of the right to anonymity within the core of the right to privacy, the tautology would deprive the latter of any specific essence or periphery with respect to data protection (*a contrario* to Article 52(1) of the Charter, and *ad absurdum* all personal data could belong to the core of the right to privacy and any de-anonymization of any data would violate the core of the right). The Court's earlier jurisprudence suggests that the object of the right to privacy is, *inter alia*, a bundle of personal data, of which some belong to its core and some do not. Both rulings in *res DRI* and *Schrems*[81] upheld the classic metadata/content distinction. Balancing *per* Article 8(2) of the Charter, guided by the Member States' discretion (Article 5(2) DPD),[82] could determine which data belongs to which category. An individualised approach is required,[83] while in particular, data sensitivity and the public interest in obtaining specific information must be taken into account.[84] In this respect, the essence of the right to private life has, *inter alia*, been found in the impermissibility of such derogations and limitations to the protection of personal data that would allow for accessing the *content* of electronic communications on a generalised basis in light of the objective of securing public protection.[85] More recent judgements, however, seem to depart from this position. The Court started to recognise that just because particular data processing concerns metadata (such as the name or IP address of a user, information on the periphery of the right to privacy) as opposed to content, it cannot be automatically concluded that such processing is permissible.[86] In *re Tele2*, the Court noted that the relationship could be far more complicated and meaningful. This accompanied a realisation of the potential for data identification that is accessible in today's Internet architecture (*re Breyer*). If ISPs are required to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment and its location, the retained data has the potential to describe with precision the private life of individuals concerned ("everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them").[87] It follows that metadata, or at least in bulk, is no less sensitive than the actual content of communications.[88] As such, it is the authors' view that the core or periphery of the right to privacy can be determined upon evaluation of the relationship between nature of the information relating to a person and the exercise of that person's autonomy in relation to that information.

20 In *re Coleman*, AG Maduro posited that the value of personal autonomy (underlying the principle of equality) dictates that "individuals should be able to design and conduct the course of their lives through a succession of choices among different valuable options". As such, the exercise of autonomy requires an array of relevant options from which to choose.[89] To be anonymous is certainly an expression of personal autonomy; it is a *means* of exercising a particular fundamental right. Indeed, there are other (equivalent) *means* of such exercise, each arising from the personal autonomy of individuals and protected under the principle of equality, unless such would amount to an abuse of law or would constitute an interference with other fundamental rights. The word "*means*" is key here. Means do not operate alone, but their character and importance must be determined with regard to upon what actions or information they are exercised. Any such *means*, expressions of autonomy, including

under the scope of the right to privacy *per* Article 8 ECHR (Kalacheva v. Russia, App No 3451/05, 7th May 2009, Tysiac v Poland, App No 5410/03, 20th March 2007, para 107 or Munjaz v the UK, App No 2913/06, 17th July 2012, para 80).

81 For a long time, other scholars have argued that systematic collection of traffic data affects the inviolable core of the right to privacy (e.g. LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens Hearing, European Parliament, 14 October 2013, Statement by Professor Martin Scheinin (EUI), former UN Special Rapporteur on human rights and counter-terrorism).

82 See e.g Judgement of the Court of 29 January 2008, Promusicae, Case C-275/06, ECLI:EU:C:2008:54, para 70. The Court insisted on the need to interpret the DPD and E-Privacy Directive so as to allow a fair balance to be struck between the various fundamental rights protected by the EU legal order.

83 Judgment of the Court of 24 November 2011, ASNEF, Cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, para 47.

84 Judgement of the Court (Grand Chamber) of 13 May 2014, Google Spain, C-131/12, ECLI:EU:C:2014:317, para 81 and similarly Delfi v Estonia, App No 64569/09, 16 June 2015, ECtHR, para 132 and Opinion of AG Bobek, delivered on 26 January 2017, C-13/16, Rīgas satiksme, ECLI:EU:C:2017:43, para 69.

85 Judgment of the Court (Grand Chamber) of 6 October 2015, Schrems, C-362/14, ECLI:EU:C:2015:650, at 94.

86 Also, in the words of ECtHR: *"[A]lthough freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others."* K.U v Finland, App No 2872/02, 2nd December 2008, ECtHR, para 49.

87 Judgment in Tele2 Sverige, ECLI:EU:C:2016:970, para 98 and 99.

88 Ibid.

89 Opinion of AG Maduro in Coleman, ECLI:EU:C:2008:61, para 9.

anonymity, could be then found on the periphery of a fundamental right. However admittedly, interfering with some *means* could pose a significant obstacle to the exercise of a fundamental right as a whole, and consequently impact upon the core of that right. To verify the impact, the wording of Article 52(1) of the Charter would dictate that any limitation, for example, of the right to anonymity, must be provided for by law, be proportionate, necessary and genuine objectives of general interest recognised by the EU or by the need to protect the rights and freedoms of others.[90] In this sense, the autonomy of some could trump the autonomy of others (as was the case, for example, in *re Österreichischer Rundfunk*, where it was held that public access to information must be accorded priority over contractual freedom,[91] or in *re Google Spain*, where it was held that the data subject's rights override, as a general rule, the interest of Internet users to access information).

21 Is it important to weigh the right to anonymity separately as a tenet of the right to privacy in any human rights analysis concerning anonymity? Yes. Such analysis helps us to reveal the relationship between the identification data and other information at issue, some of which could belong to the core of the right to privacy. This could also clarify the significance of the data at issue in respect to other fundamental rights (for example, the freedom of expression). EU law is sometimes explicit about the relationship: processing of personal data under Article 8 DPD (e.g., concerning political opinions, religious or philosophical beliefs), represents the only data processing that a Member State is allowed to exclude in a categorical and generalised manner, without the need to balance competing interests.[92] Personal data under Article 8 DPD can be processed only consensually or anonymously. This also has consequences for the right to freedom of expression. Political expression of any kind and debate of public interest benefit from the widest protection; there is very little room left to justify restrictions on political expression, unless the latter amounts to incitement to violence.[93] Nonetheless, to establish the existence of an interference with the right to privacy, it does not matter whether the information in question is sensitive.[94] Such interdependences explain why the chilling effects on the exercise of the right to freedom of expression and information (occurring through the interference with the right to privacy) only become relevant to consider when both rights are present in the analysis. If the balancing test is concerned exclusively with the primary infringements of the right to privacy, and the right to freedom of expression and information does not directly suffer, the chilling effects remain indiscernible in the analysis (e.g. in case of surveillance). *A contrario*, if the primary infringement only affects the right to freedom of expression and information, the subtle role of personal autonomy (understood as a tenet of the right to privacy) risks to stay unappreciated. This poses legal dilemmas, especially in the adjudication of ISP liability cases, where additional fundamental rights must be factored into the balance (usually the freedom to conduct a business per Article 16 of the Charter, the right to property including IP, protected by Article 17 of the Charter, and the right to a remedy guaranteed by Article 47). Juggling three or more fundamental rights simultaneously requires a robust methodology, or it may risk overlooking a particular two-sided balance.[95] Although weighing several competing interests gives the state the benefit of a wide margin of appreciation,[96] the mechanism of fair balancing must be carried out individually, on the basis of a context-dependent analysis.[97] In this respect, the Court's case law has proceeded with interesting evolutionary dynamics. In our account, the dynamics can be epitomised by the following phases:

22 (i) first, the Court established the legal framework for the imposition of an injunction *per* Article 11 of Directive 2004/48. Following this framework, as a measure designed by national law, in light of the principle of proportionality, and within the prescribed confines (Article 6 and 15(1) of the E-Commerce Directive, Article 2(3) and 3 of Directive 2004/48) must be effective and dissuasive in nature.[98] The *e-Bay* ruling, above all, modelled a particular procedure for complex balancing, which allows for factoring many conflicting interests and fundamental rights into ISP liability cases;[99]

23 (ii) the Court subsequently rejected injunctions, which involve measures combining systematic *content* analysis and processing of information connected with users' profiles[100] or IP addresses,[101]

90 Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2 Sverige, C-203/15, ECLI:EU:C:2016:970, para 94.

91 Judgment of the Court in Österreichischer Rundfunk u.a., ECLI:EU:C:2003:294, para 66.

92 Judgment of the Court in ASNEF, ECLI:EU:C:2011:777, para 48.

93 Joined App No 23927/94 and 24277/94, Sürekand Özdemir v. Turkey, 8 July 1999, ECtHR (GC), para 46.

94 Judgment of the Court in Schrems, ECLI:EU:C:2015:650, para 89.

95 Judgment of the Court in Promusicae, ECLI:EU:C:2008:54, para 65 and 66, and Judgment of the Court in Lindqvist, ECLI:EU:C:2003:596, para 85.

96 Neij and Sunde Kolmisoppi v Sweden, App No 40397/12, 19th Febraury 2013, ECtHR, part D.

97 See supra note lxxxv.

98 Judgement of the Court of 12 July 2011, L'Oréal, C-324/09, ECLI:EU:C:2011:474, para 135, 136 and 144.

99 Also see similarly K.U v Finland App No 2872/02, as discussed in Zingales N, supra note vi, p. 20.

100 Judgment of the Court in SABAM, ECLI:EU:C:2003:294, para 49.

101 Judgment of the Court in Scarlet Extended,

i.e. personal data which, in principle, allows those users to be identified;[102]

24 (iii) thirdly, the Court emphasised that a targeted injunction must seriously discourage only illicit behaviour. An example would be a prohibition imposed on an ISP to allow users to access a particular website.[103] The reasoning of the Court gives the impression that the Court does not prescribe that casting such an injunction must entail consideration of the right to privacy by default;[104]

25 (iv) finally, the Court held an injunction permissible, which dissuades the users from wrongdoing by identifying them.[105] As follows from (ii) and (iii), such a measure is targeted, if no communication content is directly analysed or blanketly monitored by an ISP. Again, in this instance users' interest in privacy has not been taken into account.

26 These phases indicate that ISP liability cases continue to be pre-occupied with the "old" content/metadata differentiation, making it relatively easier for a judge to place a final relational operator within the confines of the balancing test. Disabling anonymity certainly represents a viable alternative to enhanced content monitoring,[106] and as such, can eliminate certain doctrinal troubles with human rights dimensions. However, if a judge pursues the analysis through the unbecoming content/metadata dichotomy, and starts considering metadata (identification data) as something "merely" on the periphery of the fundamental rights, he or she becomes less concerned with the potential risk of neglecting related privacy and autonomy issues in a given case. There is a subsequent danger that the scope of the court's analysis is disproportionately narrow.

E. ISPs, the Identification Potential of Data and Data Disclosure

27 Historical experience has confirmed on numerous occasions that if a bearer of fundamental rights fears the legal, societal, or other ramifications of an exercise of these rights, he may find himself taking part in an uneasy decision between self-incrimination and self-censorship.[107] In other words, the right holder suffers from a chilling effect. In legal terms, a bearer of fundamental rights exercising this right within the confines of the law, may fear that the effect of such an exercise might either result in discrimination[108] or arbitrariness on the part of law enforcement. From the human rights perspective, it should in principle not matter whether chilling effects constitute a long-term phenomenon or, as certain research suggests, that this effect may fade away due to a growing insensitivity vis-à-vis a particular subject or practice.[109] Consensual data processing can mitigate the chilling effects to a certain extent; however, only if consent is informed and only if other equally valid choices are left for a decision maker (user) to take. Informed consent aims at eliminating an information asymmetry between a data controller and a data subject,[110] which means that the data subject should know when and to what data processing the consent is given, including an eventual data disclosure under national laws. At the same time, informed consent would not be enough if a data subject is deprived of valuable options (*means*) that would undercut his or her autonomy.[111]

28 To justify the interference with the right to information, the Court notes that a Wi-Fi network is only one of the possible ways to access the Internet. Nonetheless, in AG Szpunar's view, Wi-Fi networks are special in the sense that they offer "great potential for innovation".[112] It is therefore at least debatable whether an open public Wi-Fi or a home VDSL are equally valuable options for the exercise of the freedom of expression and information. Yet, if the main concern of personal data protection is a *large-scale* processing by mechanical, digital means, in all its varieties,[113] the analysis of the chilling effects should also be confined to this frame. Hence, while the *Mc Fadden* ruling and the national judgment that followed suit, thus far represent the only cases concerning such identification measures, the availability of choices (secured vs. unsecured networks) will eventually depend on how frequently copyright holders protect their rights via such

ECLI:EU:C:2011:771, para 51.

102 Supra note c.

103 Judgement of the Court in UPC Telekabel Wien, ECLI:EU:C:2014:192, para 42.

104 Ibid, para 47.

105 Judgment of the Court in Mc Fadden, ECLI:EU:C:2016:68.

106 Zingales N., Virtues and Perils of Anonymity Should Intermediaries Bear the Burden?, JIPITEC (2014), p. 162.

107 See also joint dissenting opinions of Judges Sajó and Tsotsoria in Delfi AS v Estonia, ECtHR judgment, notably para 3 and 14.

108 PEN's survey, Chilling Effects: NSA Surveillance Drives Writers to Self-Censor, 2013.

109 See Preibusch S., Privacy Behaviour After Snowden June Revelations, 58 Communications of the ACM.48; pp. 48-52 (2015).

110 Zuiderveen Borgesius, F. J., Improving privacy protection in the area of behavioural targeting (2014), available at: <https://pure.uva.nl/ws/files/2141324/154447_05.pdf> (accessed 15 April 2017).

111 Opinion of AG Maduro in Coleman, ECLI:EU:C:2008:61, para 11.

112 Opinion of AG Szpunar in Mc Fadden, ECLI:EU:C:2016:170, para 149.

113 Opinion of AG Bobek in Rīgas satiksme, ECLI:EU:C:2017:43, para 95.

means, and how many ISPs are forced to discontinue their services due to the costs of compliance with data protection requirements. The important implications of that are that a single infringement occurring within a particular communications network is sufficient enough to justify an injunction *per* Article 8(3) of Directive 2001/29, or Article 12(3), of the E-Commerce Directive.

29 However, from the perspective of chilling effects, it could appear more dangerous to impose an obligation upon an ISP to identify all of the network's users without the consent of the latter, following Article 7(c) DPD. For such an obligation to apply, it must be imposed by a law that unequivocally allows for its imposition and which, on its own, complies with data protection requirements, including the requirements of necessity, proportionality and purpose limitation.[114] Post *re Mc Fadden*, the proportionality of the legal obligation to collect and retain certain personal data must be tested by the judiciary, otherwise non-consensual automatic processing is inconceivable. The Court does not consider which data in particular should be collected and retained. As such, a question must be posed in relation to the principle of data minimisation *per* the DPD.[115] In this respect, it is important to note again that the contemplated identification measures should accomplish a dissuasive function. Dissuasion should be effective to such an extent as to ensure that fundamental rights would no longer be violated.[116] From the view of basic proportionality, this could only be done by requiring such identification data as would be strictly necessary for the purposes of initiating a judicial proceeding.[117] Only such identification measures, which substantially facilitate and enable the enforcement of infringed rights, would effectively dissuade potential infringers from future infringements. Because the data required to initiate court proceedings differs among the Member States, the national court must establish that the identification measure does not go beyond these data requirements. As such, assessing basic proportionality could be a mere technical issue, devoid of further judicial considerations. Further, it is important to note, as the Court did in *re Promusicae,* that the E-Privacy Directive, the E-Commerce Directive and Directives 2001/29/EC and 2004/48/EC do not oblige the Member States to impose an obligation to disclose in order to ensure effective protection of copyright. Hence, in the proportionality analysis, the obligation to identify Internet users, i.e. to collect and retain personal data, must be decoupled from the obligation to disclose, as a potential secondary legal obligation imposed upon an ISP.

30 Although the obligation of confidentiality of personal data can be restricted under the E-Privacy Directive for the protection of the rights and freedoms of others[118] (such as in the context of civil proceedings),[119] it is a matter of national law to provide a legal basis for a data disclosure.[120] In this framework, data disclosure[121] functions in the same manner as any other data processing; it must comply with the robust procedural scheme applicable to the obligation to process personal data in general. This means a fair balance must be struck[122] between multiple competing interests[123] by taking due account of the principle of proportionality. A fair balance cannot be struck, if a request for data disclosure is not substantiated and does not follow a legitimate interest. In addition to this, further safeguards must be provided: evidence of an infringement must clearly exist, information must be deemed important for the investigation, and due process must be guaranteed.[124] Undoubtedly, an interest of a (IP) right holder to sue an infringer for damages can be qualified as legitimate.[125] If a national law allows for data disclosure to protect right holders' interests in effective law enforcement, and such disclosure follows the prescribed procedural framework, which is appropriately balanced, EU law does not preclude such national legislation (*re Bonnier*). This multiple (though repetitive) procedural reasoning (at entry – data collection, data retention and at exit – data disclosure) should, in principle, guarantee that any interference with the right to privacy would bring a meaningful result after balancing. Nonetheless, if the effectiveness of identification measures is

114 Article 29 Working Party, "Opinion 15/2011 on the definition of consent" (WP 187), 13 July 2011.

115 Article 6(1)(c) and recital 28 of the DPD require that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected, but also when further processed.

116 Judgment in Mc Fadden, ECLI:EU:C:2016:68.

117 In this regard, also Opinion of AG Bobek in Rīgas satiksme, ECLI:EU:C:2017:43, para 89.

118 Judgment of the Court in Promusicae, ECLI:EU:C:2008:54, para 53.

119 Ibid, para 54.

120 See also Zingales N., supra note cvi.

121 E.g. following an order served upon an ISP to give a copyright holder an information revealing identity of a particular subscriber (an alleged infringer) per Directive 2004/48, to whom the ISP provided an IP address. Judgment of the Court (Third Chamber) of 19 April 2012, Bonnier Audio and Others, C-461/10, ECLI:EU:C:2012:219, para 36.

122 Judgment of the Court in Bonnier Audio and Others, ECLI:EU:C:2012:219, para 60 and Order of the Court of 19 February 2009, LSG-Gesellschaft, C-557/07, para 29.

123 Judgment of the Court in Bonnier Audio in Others, ECLI:EU:C:2012:219, para 58.

124 Judgment of the Court in Promusicae, ECLI:EU:C:2008:54, para 70.

125 By analogy, Opinion of AG Bobek in Rīgas satiksme, ECLI:EU:C:2017:43, at 65. At the stage of initiating legal proceedings, "*[t]he disclosure in itself would therefore not even bring about any immediate change to the legal situation of the data subject*", para 81.

evaluated only on the basis of the inevitability of prosecution and punishment of infringement of third parties' rights, assessing basic proportionality, although repetitive, appears to be an *a priori* solved problem. Secondly, there is the problem of data retention period. The idea is that personal data should in principle not be retained for longer than necessary in relation to the purpose for which they were collected or for which they are further processed. The period for which personal data can be stored must be limited to a strict minimum, and systems should be designed by default to minimize the retention period of personal information (Recital 39 of the Preamble and Article 25 of the GDPR). If the purpose of the data processing is to deflect the users from potential wrongdoing, by giving an effective possibility of initiating criminal proceedings, then the data retention period should in theory last until time for such initiation objectively lapses under national law. The data retention period is not tailored in accordance to the severity of wrongdoing, if an objective limitation period applies. However, an obligation to disclose data is not limited to a particular type of wrongdoing – let's say copyright infringement. If the permissible data retention period is not proportionately limited to the severity of the wrongdoing, but it is set objectively in accordance with the dissuasive function of the injunction – as considered by the Court – there is a risk of unjustified interference with the right to data protection. In ten years' time, new technologies can make use of current data, mandatorily stored by and ISP, in a way no one can predict. Consider only that a few years ago, that facial recognition technology was in many ways a vision of a distant future. Today, for example, every photo ever stored on a social media platform has the potential to be used for face recognition purposes. Such foresight and risk assessment of potential data uses should appear in the balancing exercise.

31 If an ISP is served with an order to secure its network and national law provides for a duty to disclose identity in court proceedings, an ISP becomes a part of the law enforcement framework. Different injunctions can be served, requiring the processing of different personal data with respect to different ISPs,[126] together making it reasonably easy to establish "the author of the crime" in criminal or civil proceedings.[127] This is an inherent consequence of the Internet's architecture with its cascade structure: mere conduit (Article 12); caching (Article 13); and hosting (Article 14 of the E-Commerce Directive). As such, even if ISPs would benefit from a differentiated and graduated approach[128] with regard to their liability, and corresponding to the robustness of their services,[129] the effective identification of the individual concerned faces shrinking technological hurdles. AG Szpunar warned that "any general obligation to identify and register users could nevertheless lead to a system of liability applicable to intermediary service providers that would no longer be consistent with [Article 15 of the E-Commerce Directive]",[130] a big leap away from the ISPs' neutrality principle.[131] In the online realm, it matters little at what level of the Internet architecture an interference with the right to anonymity appears. Effectiveness is the creed, and as the principle of proportionality dictates, the procedural rules should be designed in such a way that the court actions concerning ISP's activities could prevent and rapidly terminate any impairments of third parties' interests.[132] Article 8 of Directive 2004/48, in particular, provides for right of information with regard to potential infringement of an IPR, handled via a court order, although no prejudice shall be made to protection of confidentiality of information sources or the processing of personal data. This requires simultaneous compliance with the right to information and the right to protection of personal data.[133] It is now clear that an unlimited refusal to provide information on the basis of data protection of a third party, frustrates the right to information, and as such infringes the right to an effective remedy and the right to intellectual property.[134] Against all this pressure, the right to defend one's self, guaranteed under Article 48 of the Charter must continue to play an important part.[135]

32 The Court's approach may look odd considering that there is no specific EU legislation prescribing

126 See also Rosatti E., Intermediary IP injunctions in the EU and UK experiences: when less (harmonization) is more?, p. 17, available at <https://ssrn.com/abstract=2891042> (accessed on 7 March 2017).

127 Judgment of the Court in Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779, para 46 and 48.

128 Recommendation CM/Rec(2011)7 of the Committee of Ministers to Member States on a new notion of media (adopted on 21 September 2011) or Opinion of Advocate General Szpunar in Mc Fadden, ECLI:EU:C:2016:170, para 131.

129 Opinion of Advocate General Szpunar in Mc Fadden, ECLI:EU:C:2016:170 and Husovec M., supra note xii.

130 Opinion of Advocate General Szpunar in Mc Fadden, ECLI:EU:C:2016:170, para 143.

131 Opinion of Advocate General Jääskinen in L'Oréal, para 115.

132 Article 18 of the E-Commerce Directive and Judgement of the Court of 12 July 2011, L'Oréal, C-324/09, ECLI:EU:C:2011:474, para 133.

133 Judgment of the Court in Coty Germany GmbH v Stadtsparkasse Magdeburg, ECLI:EU:C:2015:485, para 28.

134 Ibid, paras 37-38.

135 Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market (COM(2016) 593 final), Article 13(2) also emphasizes the right of redress: "*Member States shall ensure that the service providers referred to in paragraph 1 put in place effective mechanisms, including for complaint and redress, that are available to users in case of disputes over the application of the measures referred to in paragraph 1.*".

mandatory retention of data for the purpose of enforcement of copyright in the online environment. As mentioned earlier, nation-specific information is needed to fill the final gaps; particularly as regards data retention, disclosure, and initiation of court's proceedings. Leading the proportionality analysis of identification measures enforced upon ISPs could then have the character of a mere technical exercise. However, a national judge can also fill other important lacunas left by the Court. The Court's dictum suggests the national judge must assess whether the injunction served upon the ISP would *effectively* work in the desired *dissuasive* manner. It does not finally prescribe the manner in which the judge should lead their analysis, and determine whether the contemplated measure goes or does not go beyond what is strictly necessary. The analysis can be more than technical as a matter of course. This would require the abandonment of the formalistic understanding of the basic proportionality test, and the allowance of important extra-legal considerations[136] arising from social, economic, political, and psychological particularities of each Member State. It is also possible to read this interpretation from the aim at which such an analysis should arrive, which is (soft) behavioural - "dissuasive" by nature. The national judge's role could then be prognostic, normative and diagnostic at the same time,[137] and ready to answer:

- how many local ISPs could be affected by such injunctions involving identification measures sought by third parties protecting their rights, and how many local ISPs could be compelled to discontinue offering communication networks due to mandatory compliance with the local data protection laws;

- what is the general level of trust of citizens towards law enforcement, local ISPs or IT security in a particular sector, and what is the general level of privacy awareness;[138]

- how difficult would it be to enforce the rights of right holders against alleged infringers, and what legal guarantees individuals whose data can be disclose dispose of under national law; or

- what role open Wi-Fi networks play in meaningful local civic participation, and could a fragmentation of political and social discussions occur?

33 These aspects differ dramatically from one Member State to another. Although the analysis of the national court will proceed with strong influence from the CJEU, significant room is left for a fully-fledged nation-specific contextual[139] examination. The Court acknowledged on a previous occasion that putting a complete end to the infringements of rights is an impossible goal to attain; in *re Mc Fadden*, the Court perhaps believed that by switching the default rules, there would be less space to circumvent the law in one way or another and achieve the stated goal.[140] However, targeting by dissuasion and chilling effects are very difficult, perhaps impossible, to reconcile. Dissuasive techniques are designed to constrain people's choices; *mutadis mutandis*, personal autonomy would have difficulties in finding its place in the analysis.

F. Conclusion

34 Arguments have long been heard that chilling effects represent an overstated legal argument,[141] an ephemeral phenomenon,[142] and that the procedural guarantees developed by the CJEU are sufficiently strong to protect both the interest in privacy (autonomy) and the interest in open communication and discussion. However, a stream of cautionary cases arose out of specific political and economic circumstances, for example, during the Cold War period. More recent examples include the *Schrems* case. These moments will come again, in a different form. To preserve the guarantees developed by the procedural scheme of human rights, relying on the habitual insensitivity developed by users as a justification for the reductionist analytical frame, does not seem the correct road to travel in this regard. Nor is the blind search for maximising security and efficiency in the online world.

35 Turning away from the reductionist position, any analysis should acknowledge that at the confluence of the right to private life and freedom of expression, the right to anonymity plays a role in the "cartelization" of the two rights in the online environment. It means that, under certain factual circumstances, concurrent interference

136 See Giovanella I. F., de Rosnay M. D., Community wireless networks, intermediary liability and the McFadden CJEU case, Communications Law, Bloomsbury, Wiley, 2017, 22 (1), p. 17.

137 Foucault M., Discipline and Punish, Vintage Books, 1995, p. 19.

138 Rodrıguez-Priego N., van Bavel R., Monteleone S., The disconnection between privacy notices and information disclosure: an online experiment, Econ Polit (2016) 33, pp. 433–461.

139 Ohm P., supra note lix, pp. 1762 to 1764 and Nissenbaum H., Privacy as Contextual Integrity, 79 WASH. L. REV. 119, 154 (2004).

140 Judgement of the Court in UPC Telekabel Wien, Case C-314/12, ECLI:EU:C:2014:192, para 60.

141 Penney J. W., Chilling Effects: Online Surveillance and Wikipedia Use, 31 Berkeley Tech. L.J. 117 (2016).

142 Ibid.

and remedies could be envisaged with respect to the two rights in question. Hence, strengthening or weakening anonymity in the online world affects the right to private life and freedom of expression and information simultaneously, and in the balancing exercise, these rights reinforce each other. Reductionism does not accommodate human rights in their full breadth. Therefore, one must not only recall that upholding anonymity, legally and technologically, bears the risk of unaccountable free speech, and renders the protection of the rights of third parties ineffective. To the same extent, curbing one's privacy by imposing mandatory real-identity measures, outlawing end-to-end encryption, and proliferating surveillance technologies, can severely deter an individual from the legitimate exercise of his or her right to freedom of expression and information. One must also recall that, with respect to the balancing test, the ECtHR has held that the diversity in practice among Member States as to the weighting of competing interests of respect for private life and freedom of expression calls for a wide margin of discretion, a doctrine embodying the proportionality principle,[143] and the national judge should be rightly called upon to exercise such discretion. This article argued against a purely technical reasoning, bound to lead to dismissive stance concerning extra-legal considerations, and suggested taking chilling effects seriously. Multi-level analysis of the interdependence of human rights against the backdrop of individual Member State particularities may constitute a starting point in any attempt to guide national judges in the latter direction.

143 Judgment of the European Court of Human Rights, Mosley vs UK, paras 108-110.

jipitec

Journal of
Intellectual Property,
Information Technology,
and Electronic Commerce
Law

www.jipitec.eu