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.