



CIPPM / Jean Monnet Working Papers

No. 04-2021

Robots as the New Judges:
Copyright, Hate Speech, and Platforms

Marcella Favale

July 2021



© Marcella Favale, 2021

The Centre for Intellectual Property Policy and Management of Bournemouth University is a Jean Monnet Centre of Excellence for European Intellectual Property and Information Rights (2018-2021), co-funded by the Erasmus+ Programme of the European Union.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

This Working Paper Series is peer reviewed by an Editorial Board led by prof. Ruth Towse and prof. Roger Brownsword.



This paper is licensed under a [Creative Commons Attribution-NonCommercialShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).

Robots as the New Judges: Copyright, Hate Speech, and Platforms

Marcella Favale¹

On the 16th of October 2020, a middle-school teacher, Samuel Paty, was beheaded by a terrorist who would not know of his existence if not for a number of videos posted on social media.² Yet, a law against publishing heinous content on line was approved in France on the 13th of May.³ But in June, the Constitutional Council had repealed the article requiring to take down within 24 hours the incriminated content on the basis that it would trump freedom of expression.⁴

Heated political debate has sparked on this decision in the light of the recent gruesome event. The topic of the liability of internet intermediaries has never been so contentious. Internet platforms have enjoyed immunity (known as Safe Harbour) both in EU law and overseas. More recently (2019), a new Copyright Directive⁵ entered into force. It was implemented by Member States in June 2021. This piece of legislation prompted criticism because it requires enhanced responsibility for Internet platforms that do not remove quickly enough illegal content from their social media.⁶ Currently, two new pieces of legislation are under way to horizontally streamline platforms' filtering duties (the Digital Services Act and the Digital Markets Act).⁷ However, a lot needs to be done to define the contours of these new norms, notably about different types of illegal content and whether they deserve different treatment.

This paper discusses filtering obligation (Robots as opposed to Judges) on copyright infringement vs. defamation/hate speech. It argues that it is not legally viable to implement the same norms on such different areas of law as the consequences of these norms' infringement are incomparable.

¹ Dr. Marcella Favale is Senior Research Fellow at the Centre for Intellectual Property Policy & Management (CIPPM) Bournemouth University: mfavale@bournemouth.ac.uk

² A. Poirier, 'We French love our history teachers – Samuel Paty made us remember why', The Guardian, 25/10/20 at <<https://www.theguardian.com/commentisfree/2020/oct/25/we-french-love-our-history-teachers-samuel-paty-made-us-remember-why>> (accessed 26/10/2020)

³ Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet, JORF n°0156 du 25 juin 2020, available on <<https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000038745184/>> (accessed 26/10/2020)

⁴ Conseil Constitutionnel, Décision n° 2020-801 DC du 18 juin 2020, available at <<https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm>> (accessed 26/10/2020)

⁵ Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC

⁶ Ibid, Art 17.

⁷ <<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>> (accessed 29/07/2021)

1. Platforms, Immunities, and Accountability

Communication via the Internet went a long way from its beginning. The already revolutionary scenario of twenty years ago underwent a major transformation and evolution, in a way that nobody could have anticipated.

At the incept, the global network was used to share messages and information, mainly among researchers. Then, when the Internet opened its doors to the public at large, there was a proliferation of internet “web sites”, hosted by Internet Service Providers (ISP). In some instances, content of these websites was unlawful. In these cases, right holders would pursue the infringer or claim some form of liability from the service providers. Legislators, trying to harness a totally new reality, attempted to address the issue of the liability of these providers of –often- both Internet access and web hosting.

ISP argued that by being “mere” intermediaries, they could not control the content that their subscribers were publishing online, and therefore could not be responsible for the unlawful actions taking place on their platforms.⁸ To this argument, right holders responded that intermediaries would often benefit from infringing activities. Hence, their provision of services could not be considered totally neutral and therefore intermediaries should be held accountable.⁹

Potential liability of the intermediary included: a) contributing to the infringing activities while having either actual knowledge or constructive knowledge¹⁰; b) being vicariously responsible for infringing activities by its right and ability to supervise the direct infringers and profits from the infringing activities¹¹; c) being liable for inducement of copyright infringement by intentionally engendering the infringing actions.¹²

⁸ It needs to be noted that unlawful content includes not only Intellectual Property infringement (mostly uploading unauthorized copyright content and trading in trademark counterfeit products) but also hacking, identity theft, child pornography, online gambling and other crimes

⁹ See case-law cited further below

¹⁰ Contributory liability. See *Religious Tech. Ctr. v. Netcom On-line Commc'n Serv., Inc.*, 907 F.Supp. 1361, 1376 (N.D. Cal. 1995)

¹¹ Vicarious liability. See *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001)

¹² Inducement doctrine. See *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005)

To stop internet liability issues from hindering the digital revolution, a “Safe Harbour” protection was introduced to the benefit of ISPs. Safe Harbour is a construct originated in the United States in the mid-nineties, when legislation was introduced to shelter ISP from the illegal activities of their subscribers.¹³ In Europe, few years later, the E-Commerce Directive was issued to the same end.¹⁴ It creates a set of immunities for online service providers.¹⁵ Unlike in the American legislation,¹⁶ these are broadly conceived immunities, not restricted to a specific legal subject matter, as for example copyright.

The E-commerce Directive, therefore, under certain conditions, precludes monetary damages against ISPs for the unlawful content they host. However, it is always possible for right holders to seek judiciary relief and apply for an injunction to stop the unlawful behaviour or to gather information on the infringer.

According to this piece of legislation ISPs shall not be liable for the information transmitted or stored while performing one of these activities: a) Mere conduit (art. 12); b) Caching (art. 13); and c) Hosting (art. 14). “Mere conduit” mainly refers to the provision of Internet access, which involves unfiltered and non-mediated transmission of information. “Caching” is the temporary storage of information, which is part of a technical process, “for the sole purpose of making the transmission more efficient”.¹⁷

After the E-commerce Directive, the Information Society Directive of 2001¹⁸ defined more in detail the concept of caching, as “Temporary acts of reproduction ... which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable: (a) a transmission in a network between third parties by an intermediary”. This is the only copyright Exception that Member States are mandated to implement.¹⁹

¹³ The Communications Decency Act (DCA) 1996, Sec. 230 and the DMCA (1998), Sec. 512 “Online Copyright Infringement Liability Limitation Act” (OCILLA)

¹⁴ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) Official Journal L 178 , 17/07/2000 P. 0001 – 0016, sec. 4 “Liability of intermediary service providers”(hereinafter, the E-commerce Directive)

¹⁵ Ibid, Artt. 12 to15

¹⁶ The U.S. enshrines Safe Harbour in two separate pieces of legislation, one of which specifically dedicated to copyright: the Communications Decency Act (DCA) 1996, Sec. 230 and the DMCA (1998), Sec. 512 “Online Copyright Infringement Liability Limitation Act” (OCILLA)

¹⁷ E-Commerce Directive, Recital 42

¹⁸ Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Official Journal L 167, 22/06/2001 P. 0010 – 0019 (hereinafter, the InfoSoc Directive)

¹⁹ Art 5.1 InfoSoc Directive

“Hosting” refers to storage of information (at the time when the E-commerce Directive was issued, it referred mainly to the storage of Internet websites on the ISP servers).

The activity of “linking”, which takes place when a website provides several internet addresses (URLs) leading to other websites, is not specifically included in the E-commerce Directive, whereas it is covered by the American legislation.²⁰ This void in European statutory regulation created some uncertainty. Initially, national European courts found that hyperlinking was exempted from liability,²¹ but subsequently it was considered as potentially infringing.²² Eventually, the Court of Justice of the European Union (hereinafter CJEU) has confirmed this construct: hyperlinking is not infringing²³ unless it links to infringing material and the person that provides the link has either actual or constructive knowledge that the material is infringing.²⁴

Finally, the E-commerce Directive established that ISPs have no obligation to generally monitor the information stored on their servers or to actively seek instances of illegal activities of their customers.²⁵

However, the immunity from liability for ISP that host content on their services (“hosting”) only applies on two conditions:

- First, the ISP needs not to have actual knowledge²⁶ of an illegal activity carried out on its services, or it must not be aware of facts or circumstances from which this activity is apparent.²⁷
- Second, if the ISP obtains such knowledge, it must act expeditiously to prevent access to the illegal content.²⁸

²⁰ 17 U.S. code §512(d).

²¹ See *Shetland Times Ltd. v. Wills*, 1997 SC 316 ; *Havas Numerique et Cadre Online v. Keliob*, Tribunal de commerce de Paris 26 december 2000 <https://www.legalis.net/jurisprudences/tribunal-de-commerce-de-paris-ordonnance-de-refere-du-26-decembre-2000>; *Stepstone v. Ofir*, Landgericht , Koln, February 28 2001 :28 O 692/00 ; *PCM v. Kranten.com*, Rb. Rotterdam 22 august 2000. Zaak/Rolnummer: 139609/KG ZA 00-846 ; *Danish Newspaper Publisher Association v. Newsbooster.com* [2003] ECDR 5 ; *Holtzbrinck v. Paperboy (“Paperboy”)* BGH, 17 July 2003, case I ZR 259/00

²² *Google Inc. v. Copiepresse SCRL* [2007] ECDR 5; *Public Relations consultat associations (PRCA) v. The Newspaper Licensing Agency (NLA)* [2010 EWHC 3099 ch ; see A. Murray, *Information Technology Law* 3rd ed (OUP 2016) at 276-295.

²³ C-466/12 - *Svensson e.a.* ECLI:EU:C:2014:76 ; C-348/13, *BestWater International* ECLI:EU:C:2014:2315; C-360/13 - *Public Relations Consultants Association (Meltwater)* ECLI:EU:C:2014:1195

²⁴ C-160/15 *GS Media* ECLI:EU:C: 2016:644. See also generally M. Borghi, ‘Hyperlink: la Corte Europea riscrive il diritto di comunicazione al pubblico’, *Giurisprudenza Italiana*, October 2017

²⁵ E-Commerce Directive, art. 15

²⁶ In case law this is interpreted as actual knowledge in the US whereas it is more construed as constructive knowledge in Europe. See B. M. Farano, ‘Internet Intermediaries’ Liability for Copyright and Trademark Infringement: Reconciling the EU and U.S. Approaches’, TTLF Working Paper No. 14, available at <<http://www.law.stanford.edu/organizations/programs-and-centers/transatlantic-technology-law-forum/ttlf-working-paper-series>> (accessed 05/04/2020), at 77

²⁷ E-Commerce Directive, Art. 14(a)

²⁸ E-Commerce Directive, Art. 14(b)

Interestingly, in the American legislation (which we recall only applies to copyright) other conditions are required to shelter hosting ISPs: the provider must have the right and the ability to control the allegedly unlawful activities and must have financially benefitted directly from them.²⁹

Albeit these additional conditions are not required by European legislation,³⁰ These principles, and in particular the absence of financial benefit, directly attributable to the infringing activity, have been confirmed by European case-law.³¹

While early “hosting” merely consisted of ISPs selling internet space to customers, subsequent “web portals” include corporate content -mainly advertisement- to frame customers’ content.³² In turn, this prompted a different definition of providers, more akin to news publishers. Subsequently, a new revolutionary wave of technological development brought on the scene User Generated Content tools. Blogs and social media expanded the reach of intermediaries exponentially. All these services require the installation of software applications (Apps), which require approval of End User License Agreements, which, in turn, routinely transfer content ownership/management to the platform³³: a long way from simple Internet access or server hosting.

Nowadays the ecosystem of intermediaries is composite and multi-faceted. (Information Service Providers) have been replaced by ISSP (Information Society Service Providers) which in turn have been replaced by OCSSP (Online Content-Sharing service providers). They include search engines, auction platforms, e-commerce platforms, products-comparing services, internet payment systems, self-publishing platforms, social media, etc.

²⁹ 17 U.S. code §512 (c)(1)(B)

³⁰ A form of absence of control is mentioned by Article 14.2 of the Ecommerce Directive, which states that the exemption shall not apply “when the recipient of the service is acting under the authority or the control of the provider”. But in this case the law does not refer to the control of the infringing activity. It rather seems to refer to the control of the customer. See Farano 2014, supra n 26, at 91

³¹ Paris Court of Appeal Sep. 3, 2010, eBay Inc et al. v. Parfums Christian Dior et al ; Cour de Cassation, Jan.14, 2010, Telecom Italia v. Dargaud Lombard and Lucky Comics; Cour de Cassation, Oct. 21, 2008, Sedo v. Hotels Meridien et al.; Cour de Cassation, Oct. 21, 2008 Lafesse v. Myspace. But see Cour de Cassation, Feb. 2, 2011, Nord-Ouest Production et al. v. Dailymotion (prec.) . See Farano 2014, supra n 26, at 96

³² L. Edwards, ‘Role and responsibility of the internet intermediaries in the field of copyright and related rights’ <<https://www.wipo.int/publications/en/details.jsp?id=4142&plang=EN>> (Geneva, 2011, 72 p.) at 4

³³ See generally M. Favale, E. Derclaye, ‘Copyright and Contract Law: Regulating User Contracts: the state of the art and a research agenda’, 18(1) Journal of Intellectual Property Law, University of Georgia, 67-140 (2011)

The legislation however did not catch up with the evolution of technology and related business models. The definition of “hosting” as a legal concept has been subjected to increasing strain, especially in the last decade. Therefore, the issue of the responsibility of intermediaries has received a lot of attention from international organizations and legislators.

The Organization for the Economic Cooperation and Development (OECD) has published in 2011 a comprehensive report on the regulation of ISSP (now OCSSP) worldwide. While examining this complex and relatively new problem, several issues were identified. In particular, it was asked:

- “To what extent should Internet intermediaries, which own and operate Internet platforms, be responsible for content originated by third parties using their Internet network or services?”
- “How far should responsibility remain solely with the original author, provider or party distributing unauthorised content? »
- “If intermediaries are deemed even partially responsible for the dissemination of the content or its use, should they be required to remove it or even to prevent its being made available in the first place? »³⁴

Answer to these questions involve normative solutions to clarify the interpretations of a number of concepts related with the liability of intermediaries. For example, one important issue relates to the definition of “knowledge” of the unlawful activity, which pre-empts the safe harbour protection. The CJEU, as it is often the case, stepped in to fill the interpretative gap in the landmark case *L’Oreal v. e-Bay*.³⁵

In *L’Oreal* the Court stated that ISSP are denied immunity if “aware of facts or circumstances on the basis of which a diligent economic operator” should have identified the illegality in question and declined to take appropriate action (Art 14(1)(b)).³⁶

Moreover, the Court continued, for such standard to be met, it is sufficient that the service provider could “uncover, as the result of an investigation undertaken on its own initiative, an illegal activity or illegal information”.³⁷ Interestingly, the Court advocated a certain balance in the protection of right holders and users: if on the one hand it supported

³⁴ OECD 2011 *The Role of Internet Intermediaries In Advancing Public Policy Objectives - Forging partnerships for advancing policy objectives for the Internet economy*, Part II, at 5

³⁵ Case C-324/09 *L’Oreal v. E-Bay* ECLI:EU:C:2011:474

³⁶ *Ibid.*, at 145 (6)

³⁷ *Ibid.*, at 122. See also Farano 2014 *supra* n. 26 at 83

‘preventive measures to discourage repeated infringement’, it also excluded a general duty to monitor users is search of infringement³⁸

In line with the highest European jurisprudence, some national European courts have followed similar interpretations of the concept of “knowledge”. For example, in *LVHM v. eBay* (France) eBay could not claim lack of knowledge since “as a broker, it was supposed to make sure the goods sold on its website did not infringe”.³⁹

Furthermore, in *Twentieth Century Fox et al. v. British Telecommunications (BT)*⁴⁰ (UK) the High Court found sufficient that BT had general knowledge that their services were being used to infringe copyright. Finally, in *Newzbin 2* (UK)⁴¹ “knowledge of the *use of the service* to infringe, rather than upon the infringements committed thereby” was found sufficient to determine liability.

In the latter case a test was elaborated to identify the responsibility of the provider. In practice, a list of circumstances must be examined to identify a form of “authorization by supply”. These circumstances include: The equipment used to infringe, the inevitable use to infringe; the degree of control by the supplier; and any steps taken to prevent infringement.⁴²

However, other European courts have excluded liability whenever the provider promptly acted to hinder access to the unlawful content.⁴³

This is another -well, the main - problematic concept relating to platforms’ accountability: the “expeditious” removal of the infringing content. Once the knowledge (or awareness) is obtained, according to the Directive, The ISP must act “expeditiously to remove or to disable access to the information”.⁴⁴

³⁸ Ibid, at 140. See also M. Leistner . Structural aspects of secondary (provider) liability in Europe, *Journal of Intellectual Property Law & Practice*, 2014, Vol. 9, No. 1, at 85

³⁹ This decision is from the TGI (first degree court). It has confirmed in high court. See *eBay Inc., eBay International / LVMH et autres*, Cour de cassation Chambre commerciale, financière et économique Arrêt du 3 mai 2012 (on Legalis.net)

⁴⁰ PLC: CHD 28 JUL 2011

⁴¹ *Twentieth Century Fox Film Corporation & Anor v Newzbin Ltd* [2010] EWHC 608 (Ch)

⁴² C. Angelopoulos, ‘Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe’, 3 *Intellectual Property Quarterly* (2013) 253-274., Amsterdam Law School Research Paper No. 2013-72, Institute for Information Law Research Paper No. 2013-11 2009, at 4

⁴³ For example, *SAIF v Google* (France) “the mere fact that the defendants are aware that the automatic indexation is likely to infringe copyrighted work is not sufficient to entail their liability since they are ready to “de-index” such content”. See also *Nord Ouest Production et al v. Dailymotion, UGC Images* (France), reaching equivalent conclusions. For a commentary of this case-law see Farano 2014, 2014 supra n. 26, at 83

⁴⁴ E-commerce Directive, art.14(b)

But how prompt the removal must be to be “expeditious” by law? Is this delay to be measured in terms of hours, days, weeks? In the absence of specific details from the Directive, the national courts of Europe have provided some legal interpretation. For example, in *Kewego* the Tribunal of Rome argued that some delay can be justified by either the need to acquire information about the users who uploaded the contents in question or the material removal of such contents. However, in the specific case scenario, 70 days (the time elapsed between the notice of the right holder and the removal of the controversial content by the ISP) was considered “unjustified delay”.⁴⁵ Subsequently, the Italian national authority on copyright matters (AGCOM) issued a regulation defining three working days as a limit for justifiable delay.⁴⁶ However, on a different subject matter (defamation) three days were considered insufficient by a UK court.⁴⁷

A typical starting point to calculate an expeditious removal is the notice from the right holder to the OCSSP claiming an illegal activity. In the American legislation this procedure, known as “notice and take down” is specifically regulated by copyright legislation. According to the U.S. Code the notice of infringement must meet a number of requirements detailed by the law: it has to include a digital signature; it has to identify clearly both the infringing material and the allegedly infringed copyright work; it has to include complete contact details of the claimant, and a declaration in good faith upon penalty of perjury that the information in the notice is accurate.⁴⁸

The E-commerce Directive, on the contrary, does not provide a “notice and take down” procedure. It merely encourages “voluntary agreements” to develop “rapid and reliable procedures for removing and disabling access to illegal information”.⁴⁹ In practice, this has prompted very diversified procedures of notice and take down included either in secondary legislation or in business practices. Most platforms, in addition, have their own notice and take down procedures included in their corporate policies.⁵⁰

⁴⁵ *RTI v. Kewego* (Tribunal of Rome, 14.08.2011)

⁴⁶ AGICOM, Regolamento In Materia Di Tutela Del Diritto D'autore Sulle Reti Di Comunicazione Elettronica E Procedure Attuative Ai Sensi Del Decreto Legislativo 9 APRILE 2003, N. 70, Allegato A alla Delibera n. 680/13/CONS del 12 dicembre 2013

⁴⁷ *Tamiz v Google* [2013] EWCA Civ 68

⁴⁸ 17 U.S. Code § 512(c)(3)

⁴⁹ E-commerce Directive, Recital 40

⁵⁰ See for example the Content ID policy by YouTube at

https://support.google.com/youtube/answer/9245819?hl=en&ref_topic=9282364 > (accessed 21/08/21). See also the Memorandum of Understanding on counterfeit goods at https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en (accessed 21/08/21)

France is currently the only European country to implement a statutory graduated response system towards Internet Access Providers, which is currently in force.. The initial version of the law⁵¹ was constitutionally challenged⁵² because it involved punitive measures without previous judicial scrutiny. The HADOPI 2.0⁵³ instead is based on a number of notices, first via email then via registered mail, and if the infringer persists in the infringing behaviour (within six months) the right holder can seek from the criminal judge an injunction to fine the infringer and suspend his Internet connection for a month.

In Ireland, initially, a voluntary graduated response scheme was implemented as a part of a settlement between Eircomm (the leading Irish ISP) and some large corporate right holders.⁵⁴ This scheme involves two subsequent warning notices followed by disconnection from the Internet, if the warnings are unsuccessful. On the basis of *Eircomm*, rightsholders attempted to seek an injunction to implement this scheme, initially without success.⁵⁵ Finally, in 2015 the plaintiff right holders (Sony Universal and Warner) succeeded in obtaining an injunction against UBC.⁵⁶ It is interesting to note that this is the only scheme originating from common law rather than statutes.

In the UK, the Digital Economy Act 2010, included a Code of conduct for platforms involving a graduated response (up to Internet disconnection). This code was welcomed with criticism by the platforms and users' associations, and eventually it was never implemented. Instead, the leading rightholders and platforms reached an agreement and

⁵¹ Loi no 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, called "Loi Hadopi 1" or "Loi création et internet", JORF n°0135 du 13 juin 2009 page 9666

⁵² Decision of the Constitutional Council : *Décision n° 2009-580 DC du 10 juin 2009 Loi favorisant la diffusion et la protection de la création sur internet.*, available at <<http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html>> (accessed 05/04/2021)

⁵³ Both version of the law are available at <<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432&categorieLien=id>>(accessed 05/04/2021). For a critical analysis of this legislation see N. Jondet, 'The French Copyright Authority (Hadopi): The Graduated Response and the Disconnection of Illegal File-Sharers' (August 24, 2010). Available at SSRN: <https://ssrn.com/abstract=1664509>.; see also generally C. Geiger 'Honourable Attempt but (ultimately) Disproportionately Offensive against Peer-to-peer on the Internet (HADOPI) – A Critical Analysis of the Recent Anti-File-Sharing Legislation in France' 42(4) *IIC - international review of intellectual property and competition law* (2011) 457-472

⁵⁴ *EMI v. Eircomm* [2010] IEHC 108. See also Edwards 2011, cited, at 32

⁵⁵ *EMI Records (Ireland) Limited, Sony Music Entertainment Ireland Limited, Universal Music Ireland Limited, Warner Music Ireland Limited and WEA International Incorporated v UPC Communications Ireland Limited* (High Court Case No. 2009/5472P, Unreported decision of Mr. Justice Charlton on 11th of October 2010)

⁵⁶ *Sony Music Entertainment (Ireland) Limited & Ors -v- UPC Communications Ireland Limited* (No. 1) [2015] IEHC 317. The ruling was confirmed in appeal: *Sony Music Entertainment (Ireland) Ltd. & Ors v UPC Communications Ireland Ltd.* [2016] IECA 231. See (for a commentary on the first degree ruling) G. Kelly, 'A court-ordered graduated response system in Ireland: the beginning of the end?' *Journal of Intellectual Property Law & Practice* 11 (3) (2016) 183-198

formed the Creative Content UK, which includes a Voluntary Copyright Alert Programme with a “notice and notice” procedure. This scheme involves several notices, with a largely educational purpose and no punitive measures. The programme started sending warnings to infringing users in early 2017.⁵⁷ Interestingly, a similar programme had been in force in the United States for four years, since 2013, but the American rightholders have decided not to extend it.⁵⁸ In the UK, eventually, a Digital Copyright Act was approved by the Parliament and it is in force since 2017. It includes provisions for age verifications by platforms, and filtering for adult content for Internet Service Providers.⁵⁹

Another contentious legal concept related to the activity of « hosting » is the “passive” role that the ISP need to have in order to qualify for exemptions from liability. The activity of the ISP in fact must be of a “mere technical, automatic and passive nature”, which implies that this has neither “knowledge” of nor “control” over the information which is transmitted or stored. This construct of the concept of passive role was first elaborated in the Recitals of the E-Commerce Directive,⁶⁰ and subsequently confirmed by the interpretation of the CJEU.⁶¹ European national courts have implemented this interpretation to rule either in favour⁶² or against⁶³ the immunity from liability.

One of the hottest issues surrounding internet platforms relates to the extent of their cooperation with right holders or alleged victims of illegal behaviour. Given the cost and practical difficulty of pursuing individual alleged offenders, right holders have often aimed their litigation at the intermediary/platform. The battle of the aggrieved party on the front of intermediaries has two objectives: the infringers and the infringement. On the one hand,

⁵⁷ See <<http://www.creativecontentuk.org/>> (accessed 05/04/2021). See also <<https://www.gov.uk/government/news/new-education-programme-launched-to-combat-online-piracy>> (accessed 04/04/2021)

⁵⁸ See <<https://www.eff.org/fr/deeplinks/2017/02/its-end-copyright-alert-system-we-know-it>> (accessed 04/04/2021).

⁵⁹ See < <https://www.legislation.gov.uk/ukpga/2017/30/contents>> (accessed 04/04/2021)

⁶⁰ E-commerce Directive, Recital 42: : “The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.”

⁶¹ C-236/08 *Google France v Louis Vuitton* ECLI:EU:C:2010:159

⁶² *Kaschke V Hilton* [2010] EWHC 1907 (QB), *Wikipedia* (Tribunal of Rome, 20.06.2013), *YouTube* (Court of Appeal Madrid 11/2014), *Dailymotion* (Court of Appeal Paris, 2.12.2014), *Rapidshare* (BGH, 15.08.2013)

⁶³ *Pirate Bay* (Stockholm district Tribunal, 17.04.2009, n° B 13301-06) *RTI v. Kewego* (Tribunal of Rome, 14.08.2011), *Spanish Napster* (District Court of Madrid 9.4.2014), *Newzbin* [2010] EWHC 608 (Ch)

they ask intermediaries information⁶⁴ on the identity of infringers/offenders, when they are aware that an infringement or illegal behaviour has taken place. On the other hand, they ask intermediaries help in policing the Net in search of further instances of illegal behaviours of which they are not yet aware. While the first objective has been broadly achieved before the judiciary, the second appears (at least so far) much more challenging.

The E-commerce Directive specifically stipulates that Member States cannot impose on internet intermediaries a « general obligation to monitor » their customers in search of infringing activities.⁶⁵ By general monitoring the law intends indiscriminate and preventive monitoring of all subscribers of a platform, rather than monitoring the system in search of a specific infringing activity that has been signalled by the right holder. Case-law on this subject-matter confirms the distinction, both in the EU and national courts. In *Scarlet*,⁶⁶ “monitoring all data from all customers for any future infringement for an unlimited time” was considered contrary to the applicable European Directives. Conversely, German jurisprudence found searching and removing links that infringe the plaintiff’s copyright an activity that could be required to ISP by injunction.⁶⁷ However, the German Federal High Court in 2015 clarified that albeit internet intermediaries can be held responsible for illegal content uploaded on their services by users, the claimant should first exhaust all reasonable measures to enforce their rights against the primary infringer.⁶⁸

The position of the CJEU against general filtering was subsequently confirmed in *SABAM*, where the referring court directly asked the European judges whether the directives on E-commerce, Enforcement, and Data Protection⁶⁹ preclude filtering injunctions to platforms; and the Court gave a negative answer.⁷⁰

Furthermore, when questioned whether the Data Protection Directive precludes an injunction to OCSSP to give information on subscribers in civil proceedings, the Court answered in the negative.⁷¹ Further, when the Court was asked whether the E-commerce

⁶⁴ E-commerce Directive, Art 15(2)

⁶⁵ E-commerce Directive, Art. 15 (1)

⁶⁶ C-70/10 *Scarlet Extended*, ECLI:EU:C:2011:771

⁶⁷ *GEMA v Rapidshare*, BGH, 15.08.2013

⁶⁸ See generally M. Mimler, ‘First things first: German Federal High Court provides guidance on ISP liability in online copyright infringement cases’, (2016) *Journal of Intellectual Property Law & Practice* 11 (7) 1 485–489. See Also M. Leistner, *supra* n.38, at 78

⁶⁹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281*, 23/11/1995 P. 0031 - 0050

⁷⁰ C-360/10 *SABAM v. Netlog* ECLI:EU:C:2012:85

⁷¹ C-461/10 *Bonnier audio v Perfect Communication* ECLI:EU:C:2012:219

Directive, the InfoSoc Directive,⁷² and Enforcement Directive⁷³ require OCSSP to communicate users' personal data for civil proceedings, the answer was also negative.⁷⁴ This means that Member States are allowed to implement legislation allowing requests of information also in civil proceedings, but they are not mandated to do so by European law. The reason for this approach of the CJEU is arguably to be found in the attempt to preserve the « balance of rights » of the parties involved in the copyright play.⁷⁵

If monitoring duties are clearly excluded when they are indiscriminate and are clearly allowed when they are specific, injunctions requesting OCSSPs to block access to specific websites are more controversial. The CJEU has stated that fundamental rights do not preclude an injunction to OCSSPs to block a pirate web site (*UPC Telekabel*).⁷⁶ Furthermore, injunctions requiring a provider to prevent third parties from making a copyright-protected work to the public by filtering access to their network with technological measures or password systems have been found legitimate.⁷⁷ In *McFadden*, the Court ruled as much, as long as the intermediary could choose which system to implement.⁷⁸

These wavering interpretations of legal concepts revolving around the liability of internet intermediaries are symptoms of the uncertainty caused by outdated legislation applied to a radically transformed scenario. On the one hand rights holders push for more effective measures (e.g. “notice and stay down”) and for a narrower interpretation of the “hosting” immunity. On the other hand, intermediaries claim their neutrality and fight against the increased costs of a raising liability, which threatens their business models.

Against this complex scenario and mindful to find a balance between the protection of users and businesses within the Internal Market, the EU Commission announced few years ago new copyright legislation. In May 2015, it issued a Communication on a Digital

⁷² Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society *Official Journal L 167*, 22/06/2001 P. 0010 – 0019 (hereinafter, the InfoSoc Directive)

⁷³ Directive 2004/48/EC of the European Parliament and of the C of 29 April 2004 on the enforcement of intellectual property rights *Official Journal L 157/45*, 30.4.2004

⁷⁴ C-275/06 *Promusicae* ECLI:EU:C:2008:54; C-461/10 *Bonnier Audio* ECLI:EU:C:2012:219

⁷⁵ See M. Favale, M. Kretschmenr, P. Torremans, 'Is there a EU Copyright Jurisprudence? An Empirical Analysis of the working of the European Court of Justice' 79(1) *Modern Law Review* (2016) 31-75, at 65.

⁷⁶ C-314/12 *UPC Telekabel Wien vs Constantin Film Verleih* ECLI:EU:C:2014:192

⁷⁷ C-484/14 *McFadden vs Sony* ECLI:EU:C:2016:689.

⁷⁸ *Ibid*, Judgement, at 102.6

Single Market Strategy for Europe,⁷⁹ in which it announced the intention to make “EU Copyright Rules fit for the Digital Age”. This strategy involved providing better choices and access to content online, fairer online environment for creators, and improved copyright rules for copyright exceptions. Specifically, on intermediaries, the Commission declared that [it] “will explore the need to issue Guidance on voluntary measures, to render the fight against illegal content online more effective, and in order to respond to the call for more clarity made by platforms”.⁸⁰

In September 2015, the Commission issued a public consultation on the responsibility and regulation of ISSP, whose results were published in early 2016. Answers to the consultation, unsurprisingly, revealed a lack of consensus between right holders and platforms on the extent of the latter’s liability. However, there was a consensus on the lack of clarity in the current law and on the need for updated legislation.

In December 2015, the commission issued a communication entitled “Towards a Modern Copyright Framework”⁸¹ in which it declared the intention to: a) fight mass professional infringement by ‘applying ‘follow-the-money’ mechanisms based on a self-regulatory approach’ ; b) to “clarify[...] the rules on provisional and precautionary measures and injunctions and their cross-border effect’ ; c) and to perform an ‘assessment of ‘notice and action’ mechanisms (e.g. the ‘take down and stay down’ principle) ‘.

Finally, in September 2016 the commission issued its Proposal For a new Directive on copyright in the Digital Single Market.⁸² Surprisingly, the proposal for the new Directive did not include any of the above legislative actions.

Article 13 of the Proposed Directive stipulated that ISSP (OCSSP) shall “prevent the availability on their services of works or other subject-matter identified by rightholders through the cooperation with the service providers”. In addition, the article specified what tools OCSSPs should implement to prevent this availability. Controversially, “effective

⁷⁹ Available at <http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:52015DC0192> (accessed 04/04/2021)

⁸⁰ <<https://ec.europa.eu/digital-single-market/en/liability-online-intermediaries>> (accessed 04/04/2021)

⁸¹ Available at <<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0626>> (accessed 04/04/2021)

⁸² 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)*, [Hereinafter: Proposed copyright Directive] available at <<https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-593-EN-F1-1.PDF>> (accessed 04/04/2021)

content recognition technologies” are basically mandated by the Directive, nor it helps that these technologies “shall be appropriate and proportionate”.⁸³

The Proposed Copyright Directive has raised, at the time, enormous criticism and concern among copyright literature. First, it was argued that this proposal was not based on sound empirical evidence (the impact report was not carried out because of ‘insufficient data available’). Second, a point was made that mandating “effective content recognition technologies” will distort competition, because it would be difficult for new entrants in the market to compete with OCSSPs already implementing content recognition measures (e.g. YouTube).⁸⁴ Third, the proposed Directive according to some was incompatible with the Charter of Fundamental Rights of the European Union (CFREU), with Articles 14 and 15 of the E-commerce Directive (safe harbour and no obligation to monitor), with the jurisprudence of the CJEU (*Scarlet*,⁸⁵ *SABAM*⁸⁶), and with Article 3 of the InfoSoc Directive.⁸⁷ The latter in particular raised concerns because Recital 38 of the proposed Directive assumed intermediaries as carrying out an act of communication to the public.⁸⁸ In this case, internet intermediaries would have been directly liable for copyright infringement.⁸⁹

Other criticisms⁹⁰ included the fact of being against the freedom to conduct business (Art 16 CFREU), against the freedom of information and communication (Art. 11 CFREU), and against the Enforcement Directive, which states that the measures to be taken to help

⁸³ Proposed Copyright Directive, Art. 13.1. For the critical discussion see G. Frosio, ‘Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy’ (06.02, 2017). 111 *Northwestern University Law Review Online* (2017) Forthcoming. Available at SSRN: <https://ssrn.com/abstract=2912272>

⁸⁴ European Copyright Society, ‘General Opinion on Copyright Reform’, 2017, available at <<https://europeancopyrightsocietydotorg.files.wordpress.com/2015/12/ecs-opinion-on-eu-copyright-reform-def.pdf>> (accessed 04/04/2017).

⁸⁵ C-70/10 *Scarlet Extended*, ECLI:EU:C:2011:771

⁸⁶ C-360/10 *SABAM v. Netlog* ECLI:EU:C:2012:85

⁸⁷ S. Stalla-Bourdillon, E. Rosati, K. Turk, C. Angelopoulos, A. Kuczerawy, M. Peguera, M. Husovec, ‘A Brief Exegesis of the Proposed Copyright Directive’ (November 24, 2016) Available at SSRN: <https://ssrn.com/abstract=2875296>

⁸⁸ Proposed Copyright Directive, Recital 38. “Where information society service providers store and provide access to the public to copyright protected works or other subject-matter uploaded by their users, thereby going beyond the mere provision of physical facilities and performing an act of communication to the public...”

⁸⁹ C. Angelopoulos, ‘On Online Platforms and the Commission’s New Proposal for a Directive on copyright in the digital single Market, CIPL Cambridge, January 2017, available at <https://www.civil.law.cam.ac.uk/sites/www.law.cam.ac.uk/files/images/www.civil.law.cam.ac.uk/documents/angelopoulos_platforms_copyright_study.pdf> (accessed 04/04/2021), at 17-18

⁹⁰ See generally Frosio 2017, n. 83

copyright enforcement should be not too costly and should avoid the creation of barriers to legitimate trade.⁹¹

Finally, automatic filtering device employing content recognition technologies (with are basically forms of Digital Rights Management) are likely to trump copyright exceptions, because unable to make the difference between authorised and unauthorised uses.⁹² Less critical assessments of the Proposed Copyright Directive remain a minority in the European landscape. They however also called for greater elaboration, definition, and clarification of a proposed text that neglects so many crucial points of the current scenario.⁹³

The New copyright/ Digital Single Market Directive (CDSMD)⁹⁴ entered into force on the 7th of June 2019 (to be implemented, as it did, on the 7th of June 2021). The Proposed Art 13 became Art 17, drawing on most of norms above examine. For example, it states that service providers should obtain permission from rightsholders to allow access to copyright content on its platforms⁹⁵ or they will be held accountable for the illegal uploading of infringing content on their websites unless they prove that they have made all their best effort to get rightsholders authorisation or act expeditiously upon receiving substantiated notice of infringement from right holders.⁹⁶ In doing so, intermediaries should make sure to account for the protection of some copyright exception, such as for criticism, quotation, and parody.⁹⁷ Also, they should put in place complaints and redress mechanisms that are available to users in case of disputes over the filtering.⁹⁸ General monitoring for potential infringement is excluded.⁹⁹

⁹¹ Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (*OJ L 157, 30.4.2004*) *OJ L 195, 2.6.2004*, p. 16–25, Art. 3

⁹² Frosio 2017, n. 83, at 19. For the point on DRM not respecting copyright exceptions, see also generally M. Favale, 'Fine-Tuning European Copyright Law to Strike A Balance Between the Rights of Owners and Users', 33(5) *European Law Review* (2008) 687; and also M. Favale, 'Approximation and DRM: Can Digital Locks Respect copyright Exceptions?' 19(1) *International Journal of Law and Information Technology*, (winter 2011) 306-323. In this second paper the author however argues that more recent DRM is flexible enough and the scope for potential compliance with copyright exception should be explored. In this sense see M. Favale, N. McDonald, S. Faily, C. Gatzidis 'Human Aspects in Digital Rights Management: The Perspective of Content Developers', 13(3) *Script-Ed, a Journal of Law, Technology and Society* (2016) 289-304

⁹³ ALAI France, Resolution of the 18.02.2017 on Value Gap, available at <http://www.alai.org/assets/files/resolutions/170218-value-gap-fr.pdf> (accessed 05/04/2021).

⁹⁴ Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, PE/51/2019/REV/1 *OJ L 130, 17.5.2019*, p. 92–125

⁹⁵ *Ibid*, Art 17(1)(2)(3)

⁹⁶ *Ibid*, Art 17(4)(a)(b)(c)

⁹⁷ *Ibid*, Art 17(15)(a)(b)

⁹⁸ *Ibid*, Art 17(9)

⁹⁹ *Ibid*, Art 17(8)

The final version of the Directive sparked at least as much debate as the proposal.¹⁰⁰

The "value gap"¹⁰¹ discussion around Article 17 (previously Article 13) of the CDSMD was one of the most controversial of this legislation. Platforms, according to this provision, stop benefitting from the safe harbour and are directly liable for infringing content uploaded by users. To escape this responsibility, they must obtain the authorisation from rightsholders.

¹⁰²If not, they have to: a) ensure unavailability of works for which they have obtained information from rightsholders; b) show that they have made best efforts to obtain such authorisation; c) remove allegedly infringing content expeditiously.¹⁰³ Also, a new EU Regulation¹⁰⁴ obliges platforms to remove terrorist content from their online services within one hour. This new framework applies from the 7th of June 2021.

¹⁰⁰ M. Leistner, 'European Copyright Licensing and Infringement Liability Under Art. 17 DSM-Directive Compared to Secondary Liability of Content Platforms in the U.S. – Can We Make the New European System a Global Opportunity Instead of a Local Challenge?' *Zeitschrift für Geistiges Eigentum/Intellectual Property Journal* (ZGE/IPJ) (2020) <<https://papers.ssrn.com/abstract=3572040>> accessed 17 April 2021; A. Metzger et al., 'Selected Aspects of Implementing Article 17 of the Directive on Copyright in the Digital Single Market into National Law – Comment of the European Copyright Society' (European Copyright Society 2020) ECS Opinion ID 3589323 <<https://papers.ssrn.com/abstract=3589323>> accessed 4 July 2021; S. F. Schwemer, 'Article 17 at the Intersection of EU Copyright Law and Platform Regulation' 3/2020 *Nordic Intellectual Property Law Review* <<https://papers.ssrn.com/abstract=3627446>> accessed 4 July 2021; T. Spoerri, 'On Upload-Filters and Other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market' (2019) 10 JIPITEC <<https://www.jipitec.eu/issues/jipitec-10-2-2019/4914>>; G. Frosio, 'Reforming the C-DSM Reform: A User-Based Copyright Theory for Commonplace Creativity' *IIC - International Review of Intellectual Property and Competition Law* (2020) <<https://doi.org/10.1007/s40319-020-00931-0>> accessed 4 July 2021; Maxime Lambrecht, 'Free Speech by Design – Algorithmic Protection of Exceptions and Limitations in the Copyright DSM Directive' 11 JIPITEC (2020) <<http://www.jipitec.eu/issues/jipitec-11-1-2020/5080>>; G. Spindler, 'The Liability System of Art. 17 DSMD and National Implementation – Contravening Prohibition of General Monitoring Duties?' 10 JIPITEC 334; K. Garstka, 'Guiding the Blind Bloodhounds: How to Mitigate the Risks Art. 17 of Directive 2019/790 Poses to the Freedom of Expression', *Intellectual Property and Human Rights* (4th edn, Kluwer Law International 2019) available at SSRN: <https://papers.ssrn.com/abstract=3471791>; S. Dusollier, 'The 2019 Directive on Copyright in the Digital Single Market: Some Progress, a Few Bad Choices, and an Overall Failed Ambition' (2020) 57 *Common Market Law Review* 979; Jan Bernd Nordemann and Julian Wiblinger, 'Art. 17 DSM-RL – Spannungsverhältnis Zum Bisherigen Recht?' [2020] GRUR 569; M. w< Senfleben and C. Angelopoulos, 'The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market' (October 22, 2020). Amsterdam/Cambridge, October 2020, Available at SSRN: <https://ssrn.com/abstract=3717022>; M. Husovec, and J. Quintais, 'How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms' (January 2021). GRUR International (Issue 4/2021, forthcoming), Available at SSRN: <https://ssrn.com/abstract=3463011> or <http://dx.doi.org/10.2139/ssrn.3463011>

¹⁰¹ The Transfer of Value or Value Gap issue posits that big platforms such as Youtube, Facebook, etc. do not share properly with rightsholders the revenues they generate when they allow access to copyright content. See generally M. Stedman, 'Mind the Value Gap: Article 17 of the Directive on Copyright in the Digital Single Market' (September 1, 2019). Available at SSRN: <https://ssrn.com/abstract=3810144> or <http://dx.doi.org/10.2139/ssrn.3810144>

¹⁰² Art 17 (2)

¹⁰³ Art 17(4)

¹⁰⁴ Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance) PE/19/2021/INIT OJ L 172, 17.5.2021, p. 79–109

2) Horizontal Harmonization of Monitoring Duties to Protect the User

On 15th December 2020 the EU Commission proposed two new pieces of legislation: The Digital Services Act¹⁰⁵ and the Digital Markets Act.¹⁰⁶ The aim of these new norms is to protect consumers and their fundamental rights while at the same time ensuring fair competition for businesses. To this end, it implemented the usual protocol of public consultations and impact assessments. According to the EU Commission, “The Digital Services Act significantly improves the mechanisms for the removal of illegal content and for the effective protection of users’ fundamental rights online, including the freedom of speech”¹⁰⁷ According to the text of the proposed Regulation, its aim is to “set out uniform rules for a safe, predictable and trusted online environment, where fundamental rights enshrined in the Charter are effectively protected.”¹⁰⁸ To this end, the new Regulation will establish a network of Digital Service Coordinators that will assist and supervise the enforcement of these norms within Member states.¹⁰⁹ It will establish a duty to act following an order of the judiciary,¹¹⁰ but also a system of Notice and Action for private individuals,¹¹¹ along with an internal Complaint Handling system.¹¹² Prohibition of general monitoring is confirmed by the Regulation,¹¹³ and no further precision is provided on delays for taking down allegedly illegal content beyond the usual mandate to “act expeditiously”.¹¹⁴

Among copyright scholars, Senftleben and Angelopoulos have made the argument that expressing content moderation duties across EU Directives and across different areas of law such as copyright, trademark, and defamation may prove challenging for the inherent differences among “the scope of rights and the characteristics of infringement”.¹¹⁵

¹⁰⁵ <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en> (Accessed 7/7/2021)

¹⁰⁶ <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en>(Accessed 7/7/2021)

¹⁰⁷ <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en> (Accessed 7/7/2021) at 1

¹⁰⁸ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) -hereinafter, DSA - and amending Directive 2000/31/EC, COM/2020/825 final, Art. 1(2)(b)

¹⁰⁹ Ibid, Art 67

¹¹⁰ Ibid, Art. 8

¹¹¹ Ibid, Art 14

¹¹² Ibid, Art. 17

¹¹³ Ibid, Art. 7

¹¹⁴ Ibid, Art. 5(1)(b)

¹¹⁵ Senftleben and Angelopoulos supra n 100 at 3

In the field of defamation, the CJEU established in *Glawischnig* that intermediaries must take down (by relying on automated technologies in the case of identical content) the content that has been declared illegal by the competent authority.¹¹⁶ Ms Eva Glawischnig-Piesczek was a member of the Austrian Green Party. A Facebook user shared a magazine article featuring an interview to Ms. Glawischnig with the addition of a personal comment that the referring court had found defamatory and harmful to the politician. Ms Glawischnig asked Facebook to delete this comment. Following the platform's inaction, she obtained a court injunction, after which the "post" was deleted. However, the referring court wondered whether the injunction to delete also other content on the platform, identical to the content removed, would be incompatible with the prohibition of general monitoring by art 15(1) of the E-commerce Directive, and therefore it referred the case to the CJEU. The EU Court argued that "as [it] is clear from recital 47 of that Directive [the E-commerce Dir.], such a prohibition does not concern the monitoring obligations 'in a specific case'".¹¹⁷ It is a specific case, the Court continues, when a court finds the illegal nature of a specific content, and therefore one may request the platform to remove any identical or even equivalent content, insofar as the difference is not "such as to require the host provider concerned to carry out an independent assessment of that content."¹¹⁸

However, in the recent *Peterson v. Google and YouTube*, the CJEU declared that an intermediary is held responsible if "it knows or ought to know, in a general sense, that users of its platform are making protected content available to the public illegally via its platform" [and despite that] "refrains from putting in place the appropriate technological measures that can be expected from a reasonably diligent operator in its situation in order to counter credibly and effectively copyright infringements on that platform".¹¹⁹ Moreover, the EU Court interpreted Art 8(3) of the InfoSoc Directive as not precluding national legislation to stop right holders from obtaining an injunction to remove infringing content if the platform was not aware of this infringement. In essence, EU national legislation may require right holders to notify the platform of the infringement before obtaining an injunction.¹²⁰ However, the Court states in the ruling, "it is sufficient for the rightholder to notify the service provider of an infringement in order for the latter to be required expeditiously to remove the content in question or to block access to it, and to take

¹¹⁶ C-18/18 - Glawischnig-Piesczek, ECLI:EU:C:2019:821

¹¹⁷ Ibid, at 34

¹¹⁸ Ibid, at 45

¹¹⁹ C-682/18 - YouTube and Cyando, ECLI:EU:C:2021:503, Judgement 1)

¹²⁰ Ibid, Judgement, 3)

appropriate measures to prevent further infringements from being committed, failing which the rightholder is entitled to apply for an injunction to be issued.”¹²¹

Coming back to our comparison between IP protection and defamation, therefore, while a judge order is needed to take down defamatory content, no order is routinely needed to take down copyright-infringing content and to filter further instances of the same content. In what resides the justification for this disparity? It should be, arguably, all about the balance of the fundamental rights involved, which the platform needs to respect and enforce.¹²² In cases of defamation, freedom of expression is systematically deployed as a defence, whereas in relation to copyright this is not always the case. Hence, in practice, copyright-infringing material is more likely to be expeditiously removed upon simple request of the rightsholder. While defamatory content needs to undergo the scrutiny of a Court of Law. Of course, from a practical point of view, copyright infringement is easier to detect and identify, automatically, as it mainly entails visual or audial comparison between content, whereas defamatory material, at least in its first instance, requires specific examination.

The CLIP Report of the Fordham Law School carrying out comprehensive research on defamation, harassment, and hate speech, suggested that no specific legislation exists against online hate speech and the most utilised legal remedies against this growing behaviour are lawsuits for defamation and harassment.¹²³ The report also suggests that prosecuting these cases is very difficult because of the protection, under US Law, of the First Amendment (freedom of speech).¹²⁴ Moreover, pending a court ruling on the legal or illegal nature of the speech, the platform has not a duty to act, even when the author of the content is known.¹²⁵ The sheer lapse of time allows the hateful content, potentially inciting to violence, to reverberate across the globe, unhindered. The traditional recourse to off-line justice is therefore powerless to address the most dangerous forms of this illegal behaviour, at least until expeditious remedies will be available specifically against online defamation/hate speech.¹²⁶

¹²¹ Ibid, at 140

¹²² G. Frosio, ‘Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility’ (May 28, 2017). 26(1) *Oxford International Journal of Law and Information Technology* 1-33 (2018), at 12

¹²³ A.E. Marwick, and R. Miller, ‘Online Harassment, Defamation, and Hateful Speech: A Primer of the Legal Landscape’ (June 10, 2014). Fordham Center on Law and Information Policy Report No. 2, Available at SSRN: <https://ssrn.com/abstract=2447904>

¹²⁴ Ibid, at 6

¹²⁵ C. Omer, Intermediary Liability for Harmful Speech: Lessons From Abroad, (2014) *Harvard Journal of Law & Technology* 28(1) at 318

¹²⁶ This is for example suggested by the authors of the CIPL report, supra n.123

The EU commission has undertaken soft-law strategies to address this issue. To prevent and counter the spread of illegal hate speech online, in May 2016, the Commission agreed with Facebook, Microsoft, Twitter and YouTube a “Code of conduct on countering illegal hate speech online”. The Code defined “hate speech” as “all conduct publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin”.¹²⁷ In the course of 2018, Instagram, Snapchat and Dailymotion joined the Code of Conduct. Jeuxvideo.com joined in January 2019.¹²⁸ TikTok joined in September 2020.¹²⁹ The EU Code of Conduct, is intentionally providing a response to hate speech online. Since 2016, the figures of the effectiveness of the Code of Conduct, provided by the EU Commission, suggest that on average the platforms are now assessing 90% of flagged content within 24 hours and 71% of the content deemed hate speech is removed.¹³⁰ So, terrorist content has to be removed within one hour (by EU Regulation¹³¹) while 71% of hate speech is voluntarily removed by platforms (assessed within 24 hours and presumably removed within the same timeframe). Again, we see here a difference in current practices that in theory should be harmonised in the forthcoming EU Regulations (DSA and DMA), as their vocation is to horizontally streamline moderation duties of platforms.

3) Robot vs Judge: Is this viable? And more importantly, is this recommendable?

Where does this leave us with the algorithmic moderation (e.g. robots instead of judges) of platforms? Can we possibly envisage the implementation of automatic filtering on such different case scenarios? It has been argued that automatic filtering is a good solution, indeed an ideal solution, whenever the technology will be effective enough to balance all the rights at stake.¹³² It is not difficult, given the current state of technology to conceive the implementation of an algorithm that identifies a picture, a song, a video online, which

¹²⁷ <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en> (Accessed 7/7/2021)

¹²⁹ <https://ec.europa.eu/luxembourg/news/tiktok-joins-eu-code-conduct-against-illegal-online-hate-speech_fr>(Accessed 7/7/2021)

¹³⁰ Information note - Progress on combating hate speech online through the EU Code of conduct 2016-2019 27 September 2019 (downloadable from the URL *ibid*)

¹³¹ See above, n.104

¹³² M. Husovec, ‘Remedies First, Liability Second: Or Why We Fail to Agree on Optimal Design of Intermediary Liability?’ In Giancarlo Frosio (eds.), *The Oxford Handbook of Intermediary Liability Online* (Oxford University Press 2019)

corresponds to a declared copyright-protected work. It is arguably more difficult for the algorithm to realize whether this it is a reproduction exempted from copyright protection because of criticism, quotation, or parody... but thanks to machine learning this is far from unconceivable.

However, how can we distinguish automatically from a case of political defamation, and one based on religious, ethical, racial motivation? We can assume that an algorithm can identify hate speech from vocabulary related to religion, race, sex/sexual orientation, disability. But can the right “expeditiousness” of action to be taken against potentially illegal behaviour be assessed by technological measures? Can the consequences of an illegal behaviour be assessed by a robot?¹³³ Could an algorithm have foreseen the beheading of a good high-school teacher?

Undoubtedly, some of the rules developed under current practices and jurisprudence can assist. For example, according to the proposed Regulation (DSA) expeditious treatment would be given to Notices when the information is provided by trusted flaggers;¹³⁴ and users that are likely to infringe due to recidivism will be more easily blocked.¹³⁵ Certainly, in the case of religious hate speech these norms could be successfully applied to some influential users. However, any action will have to be balanced against Freedom of Religion,¹³⁶ which is also a fundamental right.

The balance between fundamental rights seems to be key to determine the leeway of legislators in shaping these norms. In relation to copyright, the discussion on whether and to what extent freedom to carry out business should prevail on freedom of expression has been extensively debated and a consensus was reached on the need for a fair balance of rights.¹³⁷

When it comes to defamation, however, the analysis becomes more difficult. On the one hand, we have cases opposing multinationals to civil rights groups, where freedom of

¹³³ Obviously, we should also consider the possibility of AI biases. See for example generally J. A. Kroll et al, ‘Accountable Algorithms’ 2016 *University of Pennsylvania Law Review* vol 165

¹³⁴ Art 19 of Proposed DSA, supra n.108

¹³⁵ C-324/09 - L'Oréal e.a., ECLI:EU:C:2011:474, 139. See Art 20 of the proposed DSA, supra n.108

¹³⁶ Article 10 of the EU Charter of Fundamental Rights, available at <<https://fra.europa.eu/en/eu-charter/article/10-freedom-thought-conscience-and-religion>>

¹³⁷ See generally M. Favale, ‘The Right of Access in Digital Copyright: Right of the Owner or Right of the User?’, 15(1) *The Journal of World Intellectual Property*, (2012) 1-25; P. Torremans, ‘Copyright as a Human Right’, in P. Torremans (ed), *Copyright and Human Rights* (Kluwer Law International 2000); A. Lucas, ‘Droit d’auteur, liberté d’expression et droit du publique à l’information’, in A. Strowel and F. Tulkens (eds) *Droit d’Auteur et Liberté d’expression* (Larcier 2006); F. Macmillan F., ‘Towards a Reconciliation of Free Speech and Copyright’, in E.M. Barendt (ed) *The Yearbook of Media and Entertainment Law* (Clarendon Press 1996)

expression is often favoured as it underpins the social scrutiny of corporate activities potentially endangering the environment or the economy.¹³⁸ In other cases, critical forms of expression (parodies) are aimed at corporations in the framework of cultural debate.¹³⁹ On the other hand, we have defamation cases involving public figures, where freedom of expression is instrumental to a healthy democratic debate.¹⁴⁰ However, the far-reaching influence of hitherto unmoderated (or not sufficiently moderated) social media, produced defamation cases opposing private individuals on delicate topics such as religion, sex, race, disability, etc. These are defined as “hate speech” and are a potential trigger for physical violence, as the -hopefully- landmark case of Mr. Paty shows.¹⁴¹ Also, and even more dangerously, we have cases of slanderous statements conducing to social unrest and attack to democratic institutions, also producing physical violence.¹⁴² Finally, if we enlarge the picture as to include unverified statements (known as “fake news”) maliciously diffused to sway public opinion and potentially impacting on geopolitics,¹⁴³ we realize that the consequences of these different instances of illegal behaviour are simply not comparable.

This complex but also growingly concerning scenario suggests that “doing nothing” is not a conceivable option. In this sense, the initiative of the EU Commission to put forward new regulations is welcome. However, a more nuanced approach, involving a range of mandatory actions to be taken by platforms, could be more appropriate to address

¹³⁸ Some examples of a copious jurisprudence: Paris Court of First Instance, July 9, 2004, *Areva vs. Greenpeace*, PIBD 2004, No. 795, III, p. 591 see Paris Court of First Instance, January 30, 2004, *Esso vs. Greenpeace*, PIBD 2004, No. 784, III, p. 229; Communication Commerce Electronique 2004, comm. 39

¹³⁹ Also, just as examples, see the cases involving *Barbie and Mikey Mouse*; *Mattel, Inc. v. Pitt*, 229 F. Supp. 2d 315 (SDNY 2002); *Walt Disney Prods. v. Air Pirates* - 581 F.2d 751 (9th Cir. 1978) . It has been stressed by the European Court of Human Rights that multinationals claiming high damages for defamation have chilling effects on individuals and civil group attempting to criticise their policies. See *CASE OF INDEPENDENT NEWSPAPERS (IRELAND) LIMITED v. IRELAND*, Judgment (Merits and Just Satisfaction) Court (Fifth Section) 15/06/2017 , available at < <http://hudoc.echr.coe.int/eng?i=001-174419>>

¹⁴⁰ For example, some cases before the CJEU: C-201/13 - *Deckmyn and Vrijheidsfonds*, ECLI:EU:C:2014:2132; C-18/18 - *Glawischnig-Piesczek*, supra n. 116

¹⁴¹ Samuel Paty, the high school teacher beheaded by a terrorist (see n 2 above), was not the only victim of hate speech on social media. See (on the San Bernardino massacre) S. Klein and C. Flinn, ‘Social Media Compliance Programs and the War Against Terrorism’ 2016(8) *Harvard National Security Journal*. Also, The Special Rapporteur to the United Nations on Minority Issues, Dr. Fernand de Varennes, presented to the UN Forum on Minority Issues a report finding that hate and xenophobia online is spiralling and often leading to violence. See <https://www.ohchr.org/EN/NewsEvents/Pages/sr-minorities-report.aspx> (Accessed 21/08/21). See also K. Müller and C. Schwarz ‘From Hashtag to Hate Crime: Twitter and Anti-Minority Sentiment’ (July 24, 2020) available at SSRN: <https://ssrn.com/abstract=3149103> or <http://dx.doi.org/10.2139/ssrn.3149103>

¹⁴² R. Faris et al. ‘Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election’ (August 2017). Berkman Klein Center Research Publication 2017-6, Available at SSRN: <https://ssrn.com/abstract=3019414>

¹⁴³ D. Klein and J. Wueller, ‘Fake News: A Legal Perspective’ (March 8, 2017). *Journal of Internet Law* (Apr. 2017), available at SSRN: <https://ssrn.com/abstract=2958790>; Y. Benkler et al., ‘Mail-In Voter Fraud: Anatomy of a Disinformation Campaign’ (October 2, 2020). Berkman Center Research Publication No. 2020-6, Available at SSRN: <https://ssrn.com/abstract=3703701> or <http://dx.doi.org/10.2139/ssrn.3703701>

different illegal behaviours, with potentially -very- different consequences. For example, immediate action could be required from platforms to take down the most potentially dangerous content (instead of “expeditious action”). This, of course, will require a consensus on what is “most potentially dangerous” content, which of course, will prove contentious.

In conclusion, the road to horizontal harmonization of moderation duties for large platforms, albeit necessary, is complex and nuanced. Large investment in research and development will be needed in order to make technological measures capable of performing these duties.

Robots, as judges, will have to be able to assess the potential consequences of various illegal behaviour and take proportionate action in accordance. In the meantime, reliance on human judgment will be unavoidable.

Acknowledgements

I would like to thank Professor Maurizio Borghi for his insightful feedback on this paper. Please feel free to add your own input at: mfavale@bournemouth.ac.uk

Funding

This Working Paper is part of the research undertaken by the Jean Monnet Centre of Excellence on ‘European Intellectual Property and Information Rights’ at Bournemouth University (European Commission’s Erasmus+ Programme).

The funding of the European Commission to produce this publication does not constitute an endorsement of the contents, which only reflects the views of the author.