The Prohibition of General Monitoring Obligation for Video-Sharing Platforms under Article 15 of the E-Commerce Directive in light of Recent Developments: Is it still necessary to maintain it?

by **Toygar Hasan Oruç***

Abstract: The absence of a uniform notion of general monitoring, introduced under the E-Commerce Directive 2000/31/EC, leads to different interpretations of the scope and the role of the prohibition on general monitoring obligations by the EU legislators and by the Court of Justice of the European Union. While the Court of Justice of the European Union balances freedom of expression and information, right to privacy and protection of personal data and right to property on the same level of importance in determining the scope of general monitoring, this article shows that special protections attributed to the interests that are fundamental to human life and to our modern democracies under primary EU laws are ignored. Unfortunately, this further deepens the segregation in the different interpretations of general monitoring and creates an inconsistency among the recent EU legislations. The article notes that this inconsistency eventually causes a legal uncertainty for the video-sharing platforms regarding their content moderation practices and thus turning the prohibition into an empty shell. At the current stage, the article reveals the need for a clear distinction for VSPs between vertically applicable content moderation measures arising from content or sector specific regulations from the prohibition on general monitoring obligations. However, for future regulation in the EU, it is suggested to find an alternative solution to online monitoring which can suppress the impact of online illegal activities without restricting fundamental rights of individuals.

Keywords: monitoring; online; EU; intermediary; filter

Recommended citation: Toygar Hasan Oruç, The Prohibition of General Monitoring Obligation for Video-Sharing Platforms under Article 15 of the E-Commerce Directive in light of Recent Developments: Is it still necessary to maintain it? 13 (2022) JIPITEC 176 para 1

A. Introduction

1 In May 2015, the European Commission ("EC") set a goal to find how to best tackle illegal content on the Internet within the European Digital Single Market Strategy.[1] In the following year, the EC prioritised several issues relating to illegal online activities and their primary targets became, among others, the proliferation on video-sharing platforms ("VSP") of illegal content including terrorist content, child sexual exploitation, hate speech, the exposure of children and the general public to such content and the increasing inequity in the allocation of revenues generated by unlawful use of copyright-protected content between the rightsholder and VSPs.[2] The EC's Communication in 2017 marked the shifting policy discourse within the European Union ("EU") towards an enhanced responsibility of online intermediaries in the fight against these issues due to their central role in the dissemination of illegal content online.[3] The EC called, under the follow-up Recommendation, online intermediaries to adopt proactive measures and underlines the effectiveness of automated systems for the prevention of manifestly illegal content.[4]

2 On the other hand, this trend of widening the responsibility of online intermediaries in the crusade against illegal content and to ask them to implement proactive measures based on automatic filtering and detection technologies systems conflicts with the prohibition on the general monitoring obligation established under the Directive on Electronic Commerce ("ECD").[5] Although, the EC warned that the imposition of such proactive measures should respect the prohibition on general monitoring obligations, the absence of a uniform notion of general monitoring and the description of the prohibition creates legal uncertainty.[6] Particularly, while the recent EU legislations seem to require online intermediaries to implement measures to tackle the dissemination of illegal content, they also preclude those measures from leading to the ambiguous concept of *general monitoring*.[7] Therefore, this article aims to critically assess the role of the prohibition on general monitoring obligations under the evolving legislative landscape for VSPs in the EU.

3 The article starts with introducing the role of the prohibition on general monitoring within the online intermediary liability regime established under the ECD. Then, it reviews the interpretative case-law of the Court of Justice of European Union ("CJEU") concerning this prohibition and the intersection between the prohibition of general monitoring obligations and the fundamental rights protected by the Charter of Fundamental Rights of the EU ("Charter")[8] in order to identify the scope of general monitoring obligation. Chapter III discusses the interplay between the prohibition on general monitoring obligation and the recent EU legislations, the Audiovisual Media Services Directive amended in 2018 ("AVMSD")[9], the Regulation on Preventing Dissemination of Terrorist Content Online ("Terrorist Con-

* LLM, CIPP/E; Legal Counsel at Arthur's Legal B.V., Amsterdam; LLM in Innovation, Technology and the Law with Distinction, University of Edinburgh, 2020-2021. Email: toygaroruc@gmail.com. I would like to thank Joke Van Steenkiste for her continued support and Dr Paolo Cavaliere for his helpful comments on earlier drafts.

1 European Commission, 'A Digital Single Market Strategy for Europe' COM (2015) 192 final.

2 European Commission, 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe' COM (2016) 288 final.

3 European Commission, 'Tackling Illegal Content Online Towards an enhanced responsibility of online platforms' COM (2017) 555 final.

4 European Commission, 'Recommendation on measures to effectively tackle illegal content online' C(2018) 1177 final.

5 Directive (EU) 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') [2000] OJ L178/1.

6 Thomas Riis and Sebastian Felix Schwemer, 'Leaving the European Safe Harbor, Sailing Towards Algorithmic Content Regulation' (2019) 22 Journal of Internet Law 1; Maria Lillà Montagnani, 'A New Liability Regime for Illegal Content in the Digital Single Market Strategy' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) <http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198837138.001.0001/oxfordhb-9780198837138> accessed 16 August 2021.

7 Carsten Ullrich, 'Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective' (Social Science Research Network 2017) SSRN Scholarly Paper ID 3037744 <https://papers.ssrn.com/abstract=3037744> accessed 16 August 2021; Montagnani (n 7).

8 Charter of Fundamental Rights and Freedoms of the European Union [2012] OJ C 326/02.

9 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (codified version), [2018] OJ L 095/1

tent Regulation")[10] and the Directive on Copyright in the Digital Single Market ("Copyright Directive")[11]. Particularly, by analysing the permissible scope of the measures introduced under these new legislations with the CJEU's interpretation of general monitoring, the article aims at revealing the discrepancy in the implementations of the prohibition under the new EU liability regime for online intermediaries. Lastly, Chapter IV explains how this discrepancy creates legal uncertainty for the VSPs providers.

B. Understanding the Prohibition on General Monitoring Obligation

I. The Prohibition of General Monitoring Obligations under the E-Commerce Directive

4 At the EU level, the general legal framework for the online intermediary liability regime was established under the ECD in 2000. It introduced harmonised rules which apply to all providers of *information society services*, commonly referred to as o*nline intermediary services*, defined as services that are normally provided for remuneration or as a part of the economic activity, at a distance, by electronic means for the processing and storage of data upon an individual request of their user.[12] Article 14 of the ECD provides a special safe harbour regime for hosting service providers which store and host information by and at the request of their users, such as online marketplaces, social media networks, VSPs, etc. Due to its very nature, hosting services are often prone to be contaminated with illegal content uploaded by their users and therefore are subject to stricter exemption rules than other types of online intermediaries such as conduit and cashing service providers.[13] Accordingly, these providers are exempted from liabilities for the illegal content on their services uploaded by a user as long as (i) it has no actual knowledge of its user's illegal activity and is not aware of facts, and circumstances from which the illegal activities or information is apparent[14] and (ii) once it obtains such knowledge/awareness, it acts expeditiously to remove or disable access to the information.[15] This exemption is applicable only to those cases where the activity of the hosting service providers is deemed merely technical, automatic and passive which implies that the online intermediary has neither knowledge of nor control over the information which is transmitted or stored.[16]

5 This safe harbour regime is supplemented by Article 15(1) which prohibits member states from imposing general obligations on online intermediaries to monitor the information transmitted or stored on their services, or to actively look for facts or circumstances indicating illegal activity. According to the EC's Communication 'A European Initiative in Electronic Commerce' in 1997[17], the European Parliament Resolution on this Communication in 1998[18] and the First Report on the application of the ECD in 2003, this safe harbour regime including the prohibition on general monitoring obligation was rested mainly on five reasons: (i) online intermediaries, while in their infancy, lacked the technical capacity to actively and accurately monitor the massive amount of information transmitted via their services,[19] (ii)

10 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online [2021] OJ L 172/79 (Regulation on Preventing Dissemination of Terrorist Content Online).

11 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 [2019] OJ L 130/92 (The Directive on Copyright in the Digital Single Market).

12 The E-Commerce Directive, Article 2(a), Recital 18; Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, [2015], OJ L 241/1, Article 1(1)(b).

13 Edwards (n 19); De Streel and others (n 9).

14 The E-Commerce Directive Art 14(1)(a).

15 The E-Commerce Directive Art 14(1)(b).

16 The E-Commerce Directive, Recitals 42; Case C-236/08, *Google France, Google Inc v Louis Vuitton Malletier SA and Others* [2010], ECLI:EU:C:2010:159, paras 113-116.

17 The European Commission, 'A European initiative in electronic commerce. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions' COM (97) 157, 16 April 1997.

18 The European Parliament, 'Resolution on the communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on a European Initiative in Electronic Commerce (COM(97)0157 C4-0297/97)' C 167/203, 1 June 1998.

19 Commission, 'First Report on the Application of 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' COM/2003/0702 final, p 14.

such monitoring obligation was deemed unfair as it creates a burden on those acting as passive mere intermediaries,[20] (iii) a desire not to deter a developing online commerce industry in the EU with "over-regulation", (iv) the risk of over-blocking of legitimate content, i.e. free flow of information within the single market, due to the false positives of automated system or due to the tendency to avoid liability[21], and (v) the risk of creating actual knowledge and awareness which would result from an illegal content that slipped away from general proactive monitoring.[22] On the other hand, both the EC's first report as well as Recital 47 of the ECD note that this prohibition covers only the monitoring obligation in a general manner and does not include monitoring obligations in a specific case. Furthermore, it does not preclude national courts to order the online intermediary to prevent an infringement[23] nor member states to impose a duty of care to hosting service providers to detect and prevent certain types of illegal activities.[24]

6 Although, it is obvious that *monitoring* means the supervision of data traffic on the service, the ECD fails to provide guidance on the difference between the monitoring obligation "of a general manner" and "in a specific case".[25] Since the general monitoring prohibition determines the permissible scope of the measures which can be imposed on online intermediaries against illegal content, this ambiguity would likely cause problems in practice. Given that hosting service providers can still be required to prevent a specific infringement or certain illegal activities under the ECD[26], it becomes important to determine the extent of such preventive measures.[27] In fact, for the prevention of illegal content, the most effective option[28] becomes the adoption of filtering systems that monitor content either before or very shortly after it has been posted by its user.[29] Due to this ambiguity, the question as how to distinguish prohibited general monitoring obligations from permissible monitoring obligations has been addressed by the CJEU under the several preliminary rulings.

II. The CJEU's Interpretation of General Monitoring Prohibition

7 *L'Oréal v eBay* is the first case in which the CJEU assessed the compatibility of a court injunction on an online marketplace to prevent the future infringement of the trademark rights by internet users. The CJEU found that such preventive injunction would require eBay to conduct "active monitoring of all the data of each of its customers in order to prevent any future infringement" of L'Oréal trademarks and thus constitute general monitoring.[30] Instead, the CJEU suggested two measures: firstly,

20 Ibid.

21 Christophe Geiger, Giancarlo Frosio and Elena Izyumenko, 'Intermediary Liability and Fundamental Rights' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 146 <http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198837138.001.0001/oxfordhb-9780198837138> accessed 23 August 2021.

22 Edwards (n 19); Carsten Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet: Adopting the Anti-Money Laundering Framework to Online Platforms' (2018) 26 International Journal of Law and Information Technology 226; Giovanni Sartor, 'Providers Liability: From the ECommerce Directive to the Future' (European Parliament 2017) PE 614.179. <https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2017)614179> accessed 10 August 2021.

23 This conclusion is based on interpretation made by reading Recital 47 together with Article 14(3) of the ECD.

24 The E-Commerce Directive, Recitals 48.

25 Graham Smith, 'Time to Speak up for Article 15' (21 May 2017) <https://www.cyberleagle.com/2017/05/time-to-speak-up-for-article-15.html> accessed 23 August 2021.

26 The E-Commerce Directive Article 14(3), Recital 48.

27 Madiega (n 9); Martin Senftleben and Christina 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' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3717022 <https://papers.ssrn.com/abstract=3717022> accessed 21 May 2021.

28 Carey Shenkman, Dhanaraj Thakur and Emma Llansó, 'Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis' (Center for Democracy & Technology 2021) <https://cdt.org/insights/do-you-see-what-i-see-capabilities-and-limits-of-automated-multimedia-content-analysis/> accessed 18 August 2021; Sartor and Loreggia (n 9) 23 et seq. This report indicates effectiveness of automated systems for finding duplicates of identical or equivalent content to pre-identified illegal content under sufficient human supervision.

29 Aleksandra Kuczerawy, 'To Monitor or Not to Monitor? The Uncertain Future of Article 15 of the E-Commerce Directive' (*CITIP blog*, 10 July 2019) <https://www.law.kuleuven.be/citip/blog/to-monitor-or-not-to-monitor-the-uncertain-future-of-article-15-of-the-e-commerce-directive/> accessed 25 July 2021.

30 *L'Oréal SA and Others v eBay International AG and Others* [2011]

the suspension of the infringing users who sold the counterfeit L'Oréal products on the platform in order to prevent further infringements of L'Oréal's rights by the same users and secondly, the adoption of user identification measures to identify real persons behind the user accounts infringing copyrights and thus to prevent those suspended infringers from operating on the same platform under different user accounts.[31] The rationale of these suggestions is found in the analysis made by Advocate General ("AG") Jääskinen who determined double requirements of identifications of infringed right and of the infringer as an appropriate limit of a preventive measure. He opined that an injunction requiring an online intermediary to only target an infringement of the same trademarks by the same users would be permissible under Article 15(1) ECD.[32] It is argued that the CJEU's suggestions are based on this opinion since both measures require the collective application of the detection of infringement of the specific trademark and identification of specific users.[33] This means that monitoring in a "specific case" must be understood in the sense of a specific incident of infringement, i.e. infringement by the specific users, rather than in the sense of all incidents of the same trademark infringement. The latter is found to require active monitoring of all the data of each of eBay's customers, which therefore violates the prohibition on general monitoring.[34]

8 This interpretation was later tested in both the *Scarlet Extended v SABAM*[35] and the *SABAM v Netlog* cases[36] in which the CJEU discussed whether an injunction ordering a mere conduit provider and a hosting service provider, respectively, to implement a permanent filtering system to prevent infringement of specific copyright-protected works, i.e., those listed in the repertoire of the Belgian collecting society SABAM, complies with Article 15(1) ECD. The CJEU noted that the implementation of such filtering system needs three main functions: (i) to identify content that includes copyright-protected works within all the content moving through the service, (ii) to assess whether those works are used unlawfully; and, if so, (iii) blocking or removing access to the content containing such illegal use of copyright-protected works.[37] Considering these functions, the CJEU concluded that such filtering mechanism would eventually require the *active observation* of *all information* provided by *all users* and thus it would amount to general monitoring.[38]

9 This conclusion is in line with the L'Oréal judgement. Although the injunctions in both cases were targeted to specific content, i.e. L'Oréal's trademarks and SABAM's works, the CJEU considered the blanket monitoring of all activity by all users as general monitoring regardless of whether such monitoring is targeting only the infringements of specific rights. This means, due to its basic working principle, i.e., monitoring all users' content, all possible filtering measures would fall under this classic generality. In fact, this *ratione materiae* is also adopted by AG Villalón Cruz in the *Scarlet Extended v SABAM*. He stated that the implementation of filtering measures requires prior monitoring of all information and without prior monitoring, these filtering measures cannot succeed.[39] Similarly, in the *McFadden v Sony Music* case, an injunction requiring a mere conduit provider to examine all information transmitting through its internet connection services in order to prevent third parties from infringing the particular copyright-protected works of Sony is found incompatible with Article 15(1) as it would require monitoring of all information from all users.[40] According to Senftleben and Angelopoulos (2020)[41] and Kulk and Borgesius (2013)[42], the CJEU's findings in all these cases suggest that the permissible *specific* monitoring under Article 15(1) would be a filter system targeting specific, pre-notified infringements within the content posted by a specific group from among

CJEU C-324/09, 2011 I-06011 [139].

31 Ibid 141.

32 *L'Oréal SA and Others v eBay International AG and Others* [2011] CJEU C-324/09, Opinion of AG Jääskinen [181, 182].

33 Senftleben and Angelopoulos (n 32); Julia Reda, Joschka Selinger and Michael Servatius, 'Article 17 of the Directive on Copyright in the Digital Single Market: A Fundamental Rights Assessment' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3732223 <https://papers.ssrn.com/abstract=3732223> accessed 19 August 2021; Frosio (n 9).

34 *L'Oréal SA and Others v eBay International AG and Others* (n 35) para 139.

35 *Scarlet Extended v SABAM* [2011] CJEU C-70/10.

36 *SABAM v Netlog NV* [2012] CJEU C-360/10.

37 *Scarlet Extended v SABAM* (n 40) para 38; *SABAM v Netlog NV* (n 41) para 36.

38 *Scarlet Extended v SABAM* (n 40) para 40.

39 Case C-70/10 *Scarlet Extended v SABAM* [2011] ECR I– 11959, Opinion of AG Villalón Cruz, para 46.

40 Case C-484/14 McFadden v Sony Music [2016] ECLI:EU:C:2016:689, para 87.

41 Senftleben and Angelopoulos (n 32).

42 Stefan Kulk and Frederik Zuiderveen Borgesius, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2013) 34 European Intellectual Property Review 791.

all of an intermediary's users who are pre-identified as likely to share infringing content.

10 In 2019, the CJEU introduced a significant addition to this interpretation and widened the scope of permissible *specific* monitoring in the *Glawischnig-Piesczek v Facebook* case.[43] The CJEU permitted an injunction ordering a hosting service provider, Facebook, to remove content containing identical or essentially unchanged defamatory content that was previously declared illegal by a national court, "irrespective of who requested the storage of that information"[44], on condition that clear instructions must be given to the provider on how to identify such content so that it would not have to adjudicate the legality of the content.[45] For instance, any content containing the plaintiff's picture alongside a combination of certain insulting words, which have the same meaning to those used in the defamatory content, were determined as equivalent content in this context by the Austrian court. This means that to prevent the recurrence of such defamatory content, the online intermediary does not have any option but to monitor all information uploaded by all users which was explicitly rejected by the CJEU in the previous McFadden, SABAM and L'Oréal cases.

11 The reason behind this widening approach seems to be the CJEU's acknowledgement of the dynamic nature of the social network environment which allows a swift flow of the same information among its users and thus making monitoring meaningless to focus on pre-identified users.[46] Therefore, this judgement changed the scope of general monitoring, at least for defamatory cases, by allowing the active observation of all information uploaded by each service user in order to prevent *pre-identified* infringements.[47] According to the CJEU, the defining character of *prohibited* general monitoring becomes the requirements for online intermediaries to carry out an independent legal assessment of the illegal nature of the content.[48]

12 This broad interpretation was supported and the permissible scope of monitoring was further extended to copyright infringements in the *Petersons/Elsevier v Youtube/Cyando* case. The CJEU was asked whether an injunction for the removal and prevention of copyright infringing content, which exposes its addressee to unduly court costs, can be imposed on online intermediaries even if they fulfil the conditions of the safe harbour rules for hosting service providers under Article 14(1).[49] The CJEU noted that such an injunction would amount to the general monitoring obligation as it may force online intermediaries, which want to avoid court expenses, to actively monitor all the content uploaded by their users to prevent any copyright infringement.[50] However, it is allowed to impose a pre-condition for such an injunction requiring rightsholders to notify the online intermediary of an infringement prior to the commencement of court proceedings, in order to allow online intermediary to take necessary measures to prevent those notified infringements from recurrence and thus avoid being the subject of an injunction and subsequently court costs would not constitute general monitoring obligation.[51]

13 Although, the CJEU did not settle its ruling with the previous interpretation in the Glawischnig-Piesczek case, with respect to targeting copyright infringements instead of defamatory content, the AG Saugmandsgaard Øe's opinion provides a convincing reconciliation. Upon assessing the identical and equivalent content standard determined in the Glawischnig-Piesczek case in the context of copyright law, he concluded that identical content means the content that contains the exact use of the same copyright-protected work which was previously found to be infringing, whereas equivalent

43 Case C-18/18, *Eva Glawischnig-Piesczek v Facebook* [2019] ECLI:EU:C:2019:821.

44 Ibid para 37.

45 Ibid para 53.

46 Ibid 36.

47 Eleftherios Chelioudakis, 'The Glawischnig-Piesczek v Facebook Case: Knock, Knock. Who's There? Automated Filters Online' (*CITIP Blog*, 12 November 2019) <https://www.law.kuleuven.be/citip/blog/the-glawischnig-piesczek-v-facebook-case-knock-knock-whos-there-automated-filters-online/> accessed 15 August 2021; Eleonora Rosati, 'Material, Personal and Geographic Scope of Online Intermediaries' Removal Obligations beyond Glawischnig-Piesczek, C-18/18 and Defamation' (2019) 41 European Intellectual Property Review 672; Paolo Cavaliere, 'Glawischnig-Piesczek v Facebook on the Expanding Scope of Internet Service Providers' Monitoring Obligations (C-18/18 Glawischnig-Piesczek v Facebook Ireland)' (2019) 5 European Data Protection Law Review 573; Kuczerawy (n 34); Daphne Keller, 'Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling' (2020) 69 GRUR International 616.

48 Ibid 46. The CJEU notes that monitoring for identical and equivalent content which contains specific elements pre-identified by a national court would be done by automated tools and technologies without having online intermediary conduct an independent legal assessment.

49 *Frank Peterson v Youtube Inc and Elsevier Inc v Cyando AG* [2021] CJEU Joined Cases C-682/18 and C-683/18.

50 Ibid 129.

51 Ibid 136, 137.

content includes identical files that use the same work in the same way but which may have been uploaded in a different format.[52] For instance, a video showing an entire movie in a smaller screen frame on YouTube without any additional contextual information would comply with this equivalent infringing use of copyright-protected work standard.[53]

14 Moreover, the CJEU did not explain how exactly an online intermediary that previously was informed of an infringement should prevent the recurrence of that infringement. However, by analogy with the permissible duty of care obligation to prevent certain types of illegal content under Recital 48 the ECD, the CJEU's judgement can be interpreted as: online intermediaries may be forced to filter all information on their services to detect certain infringing content which is pre-identified by a national court in line with Saugmandsgaard Øe's standards. In fact, before the CJEU approved the contested condition for the preventive injunction in YouTube/Cyando case, it reiterated from the SABAM judgements that "requiring a service provider to introduce, ('...') [a] system which entails general and permanent monitoring in order to prevent any future infringement of intellectual property rights were incompatible with Article 15(1)".[54] The difference between the contested condition and this quotation is that monitoring in the former is limited with the pre-notified copyright infringement and its obligation starts upon the receipt of a notification while the injunction in SABAM cases requires monitoring of any infringements containing specific copyright-protected works which needs a contextual analysis from an online intermediary for an indefinite time. As explained in the foregoing paragraph, this conclusion also reconciles with the CJEU's approval for monitoring obligation for specific defamatory content in Glawischnig-Piesczek case.[55]

15 In the very recent ruling of *Poland v European Parliament and the Council of the European Union C-401/19* case ("Poland v Parliament and Council")[56], the CJEU confirmed this conclusion by reiterating its interpretations of general monitoring in both YouTube/Cyando and Glawischnig-Piesczek cases. The CJEU was asked to annul Article 17(4) of Copyright Directive which provides for the obligation for online content sharing services, a type of hosting service providers, to make their best effort, with high industry standards of professional diligence, to prevent the occurrence of a copyright infringement if the service providers concerned have received from the rightsholders sufficiently substantiated, relevant and necessary information of specific copyright infringement. First of all, the court concluded that requirement of best effort with high industry standards of professional diligence to prevent the occurrence of a copyright infringement obliges very large content sharing services, which receive thousands or millions of daily uploads, to carry out prior review and filtering of online content via automatic recognition and filtering tools.[57] However, the court also notes that this obligation becomes applicable only after the service provider receives *sufficiently substantiated* notice the specific infringement or *relevant and necessary* information regarding the copy-right protected work which must enable the service provider to identify the unlawful content without conducting legal assessment.[58] Lastly, once again the court pointed out that generally the service providers "cannot be required to prevent the uploading and making available to the public of content which, in order to be found unlawful, would require an independent assessment of the content by them in the light of the information provided by the rightholders and of any exceptions and limitations to copyright ('...')" as this leads to general monitoring obligation.[59]

16 The CJEU's recent clarification of general monitoring obligation confirms that any obligation to online intermediaries requiring filtering all the information on their services to detect and remove the illegal content on condition that the identification of such content must not require "an independent assessment" or "legal examination". This means online intermediaries should not be required, for example, to carry out a contextual analysis of content that contains the defamatory content pre-identified by a court but in a significantly different context or which includes a copyright protected work used in such a way that contrast the information provided by rightsholders with applicable copyright exceptions.[60] In line with Saugmandsgaard Øe's opinion in both the Poland v Parliament and Council case

52 *Frank Peterson v. Youtube Inc and Elsevier Inc. v. Cyando AG* Joined Cases C-682/18 and C-683/18 Opinion of the AG Saugmandsgaard ØE, 16 July 2020.

53 Reda, Selinger and Servatius (n 38) 17.

54 *Frank Peterson v. Youtube Inc and Elsevier Inc. v. Cyando AG* (n 49) para 135.

55 Reda, Selinger and Servatius (n 38).; *Eva Glawischnig-Piesczek* (n 24) paras 45-46.

56 Republic of Poland v European Parliament and Council of the European Union [2022] CJEU C-401/19.

57 ibid 54.

58 ibid 89–90.

59 ibid 90.

60 Republic of Poland v. European Parliament and Council of the European Union, Case C-401/19 Opinion of the AG Saugmandsgaard ØE, 15 July 2021, para 198.

and the Youtube/Cyando case, the CJEU seems to agree that any obligation to implement upload filters against manifestly illegal content, the illegal nature of which either is clear and obvious to a reasonable person or has been previously determined by a court, does not constitute general monitoring obligation.[61]

III. Intersection with Fundamental Rights and Freedoms

17 Within its interpretative case-law, the CJEU noted that while the monitoring obligations generally aim to protect the rights and interests of the people, e.g. the right to intellectual property[62], the right to reputation[63] from the infringements by internet users, it also burdens the internet users' rights to privacy and data protection, freedom of expression and information and the online intermediary's freedom to conduct a business under Articles 8, 11, and 16 of the Charter respectively.[64] In the face of this clash, the CJEU developed a *fair balance* test to strike the balance between these competing rights and interests within the framework of the online intermediary liability regime. The analysis of the CJEU's fair balance test would present how permissible *specific* monitoring obligations can be implemented. The justification for the imposition of liability on online intermediaries is supplemented by the context of the rulings of the European Court of Human Rights in which freedom of expression and information are balanced against the right to privacy in reputation.[65]

18 Apart from these fundamental rights, scholars have also raised concerns over the negative impacts of automated monitoring systems on the internet users' rights to equality and non-discrimination due to inherent bias in algorithms and thus the absence of the rights to a fair trial and effective remedy of those whose online expression is restricted by the over-blocking.[66] As both of these issues are discussed by the CJEU and AGs in relation to the risk of *over-blocking* of the users' legitimate expressions, this section will evaluate the impact on these two fundamental rights under the CJEU's fair balance test for freedom of expression and information and then the suitability of the balancing approach in the context of general monitoring of online content will be questioned below.

1. Striking a Fair Balance Between the Fundamental Rights

19 In the Promusicae case, the CJEU acknowledged that the provisions of ECD must be interpreted in such a way that it strikes a fair balance between different fundamental rights involved.[67] In the following L'Oréal case, after finding the double targeting preventive measure compatible with Article 15(1) ECD, the CJEU noted that a fair balance must be

61 Ibid.

62 *L'Oréal SA and Others v eBay International AG and Others* [2011] CJEU C-324/09, 2011 I-06011; *Scarlet Extended v SABAM* [2011] CJEU C-70/10; *SABAM v Netlog NV* [2012] CJEU C-360/10; *Frank Peterson v. Youtube Inc and Elsevier Inc. v. Cyando AG* (n 49); *Republic of Poland v. European Parliament and Council of the European Union* (n 56).

63 *Eva Glawischnig-Piesczek* (n 24)

64 *Scarlet Extended v SABAM* (n 14) paras 48, 50, 52; *SABAM v Netlog NV* (n 15) paras 47-48; *Peterson/Elsevier v Youtube/Cyando* (n 47) para 138.

65 The ECtHR has discussed, in multiple disputes, whether a hosting service provider should be liable for user-generated content and obliged to monitor and filter proactively its networks to avoid liability. Although the ECtHR's role as adjudicator of the European Convention on Human Rights ("**ECHR**") does not include to interpret EU laws, its rulings concerning the human rights-based limits on monitoring in the context of online intermediary liability still are relevant for current policy discussions on monitoring obligation in the EU. Because Article 51(3) of the Charter indicates that the meaning and scope of the rights that are protected both in the Charter and the ECHR should be the same, unless the Charter provides more extensive protection and thus ECHR-based fundamental rights constitute an integral element in the EU's constitutional order. Therefore, this section will use the ECtHR's case-law to understand the role of fundamental rights in general monitoring prohibition.

66 Robert Gorwa, Reuben Binns and Christian Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7 Big Data & Society 10,11 <https://doi.org/10.1177/2053951719897945> accessed 2 April 2021; Keller (n 52) 617; Reuben Binns and others, 'Like Trainer, Like Bot? Inheritance of Bias in Algorithmic Content Moderation' in Giovanni Luca Ciampaglia, Afra Mashhadi and Taha Yasseri (eds), *Social Informatics* (Springer International Publishing 2017); Christophe Geiger and Bernd Justin Jütte, 'Platform Liability under Article 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match' (2021) 70 GRUR International 517. Based on several studies, it is noted that automated filtering systems have unequal impacts on different populations is it will inevitably have to privilege certain formalisations of offence above others and disproportionately silence lawful of certain groups.

67 Case C-275/06, *Promusicae v Telefónica de España SAU* [2008] ECLI:EU:C:2008:54, para 63.

struck when implementing these measures.[68] In the very recent Poland v Parliament and Council case, the CJEU clarified how to carry out a fair balance test when a legal obligation targeting protection of right to intellectual property clearly entails a limitation on the exercise of the right to freedom of expression and information.[69] Pursuant to these three judgements, it is evident that even though the monitoring obligations satisfy the specificity standards as discussed in preceding Section II, they must still not constitute an excessive restriction on the fundamental rights.

a) Online Intermediary's Freedom to Conduct a Business

20 In the SABAM cases, the CJEU ruled that an injunction requiring an online intermediary to install filtering systems, at its own expenses, to monitor all the electronic communications to filter any copyright infringement, fails to find a right balance between the intermediary's freedom to conduct a business and the right to intellectual property. It noted that such system would be too sophisticated since it targets infringements of not only existing works, but also of future works that have not yet been created.[70] Therefore, obliging online intermediaries to implement such a complex system for an unlimited time was found to be an unproportionate burden on their business.

21 Similarly, in the later *UPC Telekabel v Constantin* case, the CJEU noted that imposing an open-ended injunction requiring a mere conduit provider to block access to a website with copyright infringing content would constitute a burden as it requires an online intermediary to implement complex technical solutions that would result in significant costs and have a considerable impact on the organisation of the online intermediary's activities.[71] On the other hand, the CJEU noted that it would strike a fair balance between the right to intellectual property and the intermediary's freedom to conduct business under certain conditions. First, the online intermediary must be given the freedom to choose how to block specific content in proportion to its resources and abilities.[72] Secondly, the measure implemented by an intermediary must be reasonable in light of the technical and financial capacity of that intermediary, and capable of making it difficult to commit an illegal act by internet users.[73]

22 Although the CJEU did not conduct a detailed fair balance test in the Glawischnig case, the AG Szpunar's opinion may provide some guidance. Accordingly, imposing the obligation to monitor all information in order to filter the content identical to those previously identified as defamatory content by the court would not require sophisticated technology and therefore would strike a fair balance between intermediaries' freedom to conduct a business and the right to reputation.[74] On the other hand, he warned that extending the scope of monitoring from identical to the equivalent content would not be compatible with the fair balance test. This was because the monitoring obligation to target equivalent content would require contribution of the provider in the legal assessment of the content and thus, it would be costly and require sophisticated solutions for the intermediary to develop.[75] The CJEU seemed to share the AG Szpunar's concern over the legal assessment requirements in its judgement as it concluded that the scope of monitoring must be limited with the content containing properly identified specific elements which can recourse to automated search tools and technologies and thus will not require further an independent assessment of the provider.[76]

23 In the YouTube/Cyando case, AG Saugmandsgaard ØE took a similar position by noting that a sufficiently precise or adequately substantiated notification regarding a copyright infringement enables the online intermediary to detect the infringing nature of the content without conducting a legal examination and therefore any monitoring obligation targeting such infringement would not constitute a burden on the intermediary's freedom to conduct a business.[77] In line with the Telekabel judgement, he warned that imposition of such monitoring obli-

68 *L'Oréal SA and Others v eBay International AG and Others* (n 10) para 143.

69 *Republic of Poland v. European Parliament and Council of the European Union* (n 56).

70 *Scarlet Extended v SABAM* (n 14) paras 47,48; *SABAM v Netlog NV* (n 15) paras 46, 47.

71 C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH* [2014] ECLI:EU:C:2014:192 (UPC Telekabel case), para 50.

72 Ibid paras 51, 52.

73 Ibid paras 59, 60.

74 Case C-18/18, *Eva Glawischnig-Piesczek v Facebook* [2019] ECLI:EU:C:2019:821, Opinion of AG Spunzar, paras 62, 63.

75 Ibid paras 73, 74.

76 *Eva Glawischnig-Piesczek* (n 24) para 47.

77 Joined Cases C-682/18 and C-683/18, Peterson/Elsevier v Youtube/Cyando [2021] ECLI:EU:C:2021:503, Opinion of the AG Saugmandsgaard ØE, paras 188,189,194, 221.

gation must be proportionate with the available resources of the providers since not all service providers have the necessary technical and financial resources to implement it.[78] It is not clear how the CJEU applied this proportionality requirement in its judgement. However, considering that the CJEU found YouTube's Content ID[79] as an "appropriate technological measure" to counter effectively infringements of pre-identified copyrights on intermediary service,[80] it can be argued that filtering obligations on financially and technically resourceful online intermediaries, like YouTube, against pre-identified illegal content that are capable of being identified solely by automated means, will not constitute a burden on their freedom to conduct a business. Because first, such an automated monitoring system will not be too sophisticated as no contextual judgement is required and second, its development costs would be proportionate in accordance with available resources. This interpretation also aligns with the CJEU's emphasis on automated tools in the Glawischnig judgement as well as in the Poland v Parliament and Council judgement.[81]

b) Internet Users' Freedom of Expression and Information

24 Secondly, in both the SABAM cases and in the Poland v Parliament and Council case[82], the CJEU noted that requiring providers to implement an ex-ante filtering system *could* limit the users' freedom of information, because the technology may not adequately distinguish legal content from illegal ones, so its application could lead to the blocking of legal communication.[83] Likewise, the Telekabel judgement noted that in order not to unnecessarily deprive internet users of the possibility of lawfully accessing the information available, any blocking measures must be *strictly targeted* so that the rights of non-infringing users should not be affected.[84] This reasoning also explains the rationale behind the double identifications requirement in the L'Oréal judgement. More importantly, the CJEU requires that internet users whose information at risk of over-blocking should be given *locus standi* to defend their rights in order to legitimately restrict users' freedom of expression and information.[85]

25 AG Spunzer, in the Glawischnig case, opined that imposing a filtering obligation for pre-identified specific content would not impair the internet users' freedom of expression if it does not require the active participation of the intermediary in legal assessment of the content.[86] Because this poses a risk of losing the liability exemption under the ECD, online intermediaries would be inclined to remove the content on which they cannot ensure its illegality and therefore, would end up with systematically restricting internet users' freedom of expression and information.[87] Perhaps, the CJEU's explicit emphasis on the use of an automated system which does not require an independent assessment by the provider for the filtering of defamatory content[88] could be the result of the same concern. Interestingly, the CJEU made no point on the over-blocking risk caused by the inaccuracy of filtering technologies as it was the issue in the SABAM cases. Possibly, in these judgments, the CJEU shared the opinion of AG Szpunar on that the current technology can distinguish the reproduction of identical unlawful content, which had been pre-identified and notified to the service provider, from other lawful communications.[89]

26 Similarly, in line with AG Saugmandsgaard ØE emphasis on the risk of "over-removal"[90], the YouTube/Cyando judgement highlights the importance of the provider's neutrality in the decision-making process and thus requires that any notification of an infringement must "contain sufficient information to enable" the online intermediary "to satisfy itself, without a detailed legal examination, that the content is illegal, and its removal is compatible with freedom of expression".[91] This interpretation is fur-

78 Ibid paras 195, 222.

79 'How Content ID Works' (*YouTube Help*) <https://support.google.com/youtube/answer/2797370?hl=en-GB> accessed 23 June 2021.

80 Ibid 94, 102.

81 *Republic of Poland v. European Parliament and Council of the European Union* (n 56).

82 ibid.

83 *Scarlet Extended v SABAM* (n 14) para 52; *SABAM v Netlog NV* (n 15) para 50.

84 *UPC Telekabel Wien GmbH v Constantin Film* (n 41) paras 55, 56.

85 Ibid 57.

86 *Eva Glawischnig-Piesczek v Facebook*, Opinion of AG Spunzar (n 44), para 65.

87 Ibid 73-75.

88 *Eva Glawischnig-Piesczek v Facebook* (n 24) para 46.

89 Case C-18/18, *Eva Glawischnig-Piesczek v Facebook* [2019] ECLI:EU:C:2019:821, Opinion of AG Spunzar, para 61.

90 *Peterson/Elsevier v Youtube/Cyando,* Opinion of the AG Saugmandsgaard ØE (n 48) para 189,243, 244.

91 *Peterson/Elsevier v Youtube/Cyando* (n 28) para 116.

ther confirmed by CJEU in the Poland v Parliament and Council case. Before applying the fair balance test, the court acknowledged that the use of automatic recognition and filtering tools, such as digital fingerprinting technology, become the only means to comply with monitoring obligation targeting to prevent occurrence of pre-identified infringements for certain online intermediaries hosting a large amount of content being uploaded on daily basis.[92] Furthermore, the court has confirmed that this monitoring and filtering method, by default, restricts an important means of disseminating online content and thus constitutes a limitation on the right to exercise freedom of expression and information of the users of those online intermediaries.[93]

27 Recognising the limitation on this fundamental freedom by monitoring obligations, the CJEU carried out a balancing test between the freedom of expression and information of internet users and the right to intellectual property of the rights holders. Accordingly, in addition to the provision of sufficient information to service providers as determined in the YouTube/Cyando judgement, the CJEU stated that two of the following preconditions must also be satisfied: i) the users of those service providers must be informed about prohibited contents as well as the functioning of automatic recognition and filtering systems in place, and ii) there must be an effective and expeditious complaint and redress mechanisms for users whose content was wrongly disabled or has been wrongly removed, and any complaint must be processed without undue delay and subject to human review.[94]

28 The ECtHR, has also consistently recognised the crucial role of online intermediaries for the internet users' freedom of expression as a provider of an unprecedented platform for "the free exchange of information and ideas".[95] In fact, in *Yildirim v Turkey* which involved the incidental shutting down of Google and third-party websites as a result of an interim Turkish court order targeting a website that was the subject of domestic criminal proceedings, the ECtHR, found a violation of freedom of expression and information by recognising that the internet has become one of the principal means by which individuals exercise not only their right to express their ideas but also their rights to receive information.[96] Like the CJEU's position, the ECtHR also acknowledged that compelling intermediaries to find and remove all illegal content online that is often legally disputed would force them to limit the ability to impart and receive information of ordinary Internet users and thus would have a chilling effect on their freedom of expression.[97]

29 In the *Delfi v Estonia* case, the ECtHR ruled that the imposition of the monitoring obligation against an online intermediary to filter specific illegal content, i.e. hate speech and incitement to violence, would not violate freedom of expression and information so long as the targeted illegal content is clearly identifiable in such a degree that "the establishment of their unlawful nature did not require any linguistic or legal analysis since the remarks were ('....') manifestly unlawful.".[98] In the following year, the ECtHR noted that expecting online intermediaries to take measures against unlawful online amounts to "requiring excessive and impracticable forethought capable of undermining freedom of the right to impart information on the internet" in *MTE and Index v Hungary* case.[99] Although the ECtHR assessed the impact on the intermediary's freedom instead of its users in the Delfi case, the MTE and Index v Hungary case and following cases showed that the same consideration is also applied for the balancing test with internet user's freedom of expression.[100] Perhaps, this position can be reconciled with the CJEU's concern over the *independent legal assessment* of content by providers. It seems that both European courts accepted the fact that without providing well defined illegal content, intermediaries would start systematically removing offensive, criticising, or even injurious but still lawful expression in order to avoid liability.

30 Additionally, the ECtHR also assessed the potential impact of illegal content as another parameter that

92 *Republic of Poland v. European Parliament and Council of the European Union* (n 56) para 54.

93 ibid 55.

94 ibid 88, 94.

95 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* [2016] ECtHR 22947/13) [61]; *Payam TAMIZ v the United Kingdom* [2017] ECtHR 3877/14 [87]; *Ahmet Yildirim v Turkey* [2012] ECtHR 3111/10; *Vladimir Kharitonov v Russia* [2020] ECtHR 10795/14; *Jezior v Pologne* [2020] ECtHR 31955/11.

96 *Ahmet Yildirim v Turkey* [2012] ECtHR 3111/10.

97 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* (n 88) para 86; *Rolf Anders Daniel Phil v Sweden* [2017] ECtHR 74742/14 [35]; by analogy, *Kablis v Russia* [2019] ECtHR 48310/16, 59663/17; *Ahmet Yildirim v Turkey* [2012] ECtHR 3111/10.

98 *Delfi AS v Estonia* [2015] ECtHR 64569/09.

99 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* (n 88).

100 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* (n 88) paras 91; *Rolf Anders Daniel Phil v Sweden* (n 13), Para 31; *Payam TAMIZ v the United Kingdom* (n 74) paras 80-81.

needs to be considered for the justification by the national court for restricting the intermediary's and users' freedom of expression.[101] Therefore, in case of the imposition of monitoring obligation against manifestly unlawful content, the size and reach of that online intermediary must also be taken into account for the balancing exercise.[102] In *MTE and Index v Hungary* case, the ECtHR concluded that large online platforms which run on a commercial basis and as part of their business model, try to attract a large number of users engagement should have a higher level of duty and responsibility because any unlawful content published on such platform has significantly more detrimental effect than other content on amateur or non-commercial websites or blogs.[103] The Court again applied this criteria in *Phil v Sweden*, where defamatory content was also published on a blog run by a small non-profit association.

31 In *Tamiz v UK* where a defamatory content published on Blogger.com, an online blog-publishing platform run by Google and reaching a wide audience, the ECtHR further elaborated this criteria by separating hosting service providers that do not provide any online content and merely host internet user's posts or which are private persons running a website or blog as a hobby from other platforms which actively compete for users' interaction and attention through notifications, invitations or other stimulus online and thus should bear more responsibility for user's illegal content.[104] Similarly, in the *Høiness v Norway* case that arose from a defamatory content published on a debate forum—a part of a news portal running on a commercial basis and which produces content to attract user interaction—the ECtHR again held that expecting a reactive approach from online intermediary against defamatory content, instead of proactive one such as upload filters, is proportionate limitation on freedom of expression and information.[105] Lastly, *Jezior v. Poland*, where the court applied this criteria to a defamatory content published on a privately run blog with a limited local scope and where an online intermediary which was notified of such content failed to prevent the reoccurrence, reaffirms that imposing the liability of internet user's manifestly unlawful content to an online intermediary which runs on non-commercial basis constitutes an unjustified limitation on the right to exercise of freedom of expression and information online.[106]

32 Perhaps, this soft approach on online intermediary regarding defamatory content is related to the contradictory and subjective nature of defamation cases, identification of which requires legal assessment by national courts in accordance with the national legislation.[107] Although, this issue was not explicitly discussed by the CJEU within the above-mentioned case-law, given the binding effects of the ECtHR's rulings[108], the article considers the potential reach of negative impacts of illegal content for the determination of the permissible scope of online monitoring.

33 One of the last criteria of ECtHR's fair balance exercise between freedom of expression and information of internet users and others' rights and freedoms is the availability of sufficient safeguards against the risk of over-blocking of lawful content. Although, the website blocking measures applied by a regulatory authority are discussed in both *Ahmet Yildirim v Turkey* and *Vladimir Kharitonov v Russia* cases as a prior restraint without being ordered by a court, the ECtHR noted that legitimate online blocking measure is likely to result in over-blocking and therefore requires an adequate safeguard.[109] It should be noted that the requirement of appropriate safeguard to be put in place against blocking measures is also adopted by the CJEU in Poland v Parliament and Council when defining lawful monitoring practices.[110]

34 In light of this, one can conclude that monitoring obligations that do not require legal assessment of online intermediaries for the identification of manifestly illegal content, supported by an effective redress mechanism for users whose content will be subject to such monitoring and imposed only for those intermediaries whose service reach might enable illegal content cause extensive damage do not

101 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* (n 88); *Rolf Anders Daniel Phil v Sweden* (n 89); *Payam TAMIZ v the United Kingdom* (n 88).

102 Giancarlo Frosio and Sunimal Mendis, 'Monitoring and Filtering: European Reform or Global Trend?' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) <http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198837138.001.0001/oxfordhb-9780198837138> accessed 10 August 2021.

103 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* (n 88).

104 *Payam TAMIZ v the United Kingdom* (n 88) para 85.

105 *Høiness v Norway* [2019] ECtHR 43624/14.

106 *Jezior v. Pologne* (n 88).

107 *Axel Springer AG v Germany* [2012] ECtHR 55, 6.

108 For explanation, please see fn 66.

109 *Ahmet Yildirim v. Turkey* (n 88); *Vladimir Kharitonov v. Russia* (n 88).

110 *Republic of Poland v. European Parliament and Council of the European Union* (n 56) para 94.

violate the freedom of expression and information of both internet users and online intermediaries.

c) Internet Users' Rights to Privacy and Protect Personal Data

35 Finally, blanket filtering and monitoring obligations have a serious impact on the internet user's right to protection of personal data.[111] When the CJEU was drawing the permissible scope of filtering in the L'Oréal case, it warned that in order to protect privacy and personal data of ordinary users, any identification measures should be taken against those internet users operating in the course of trade and not in a private matter.[112] Likewise, in the *SABAM v Netlog* case, the CJEU noted that the installation of a filtering system which indiscriminately monitors all information would *de facto* require the identification, systematic analysis, and processing of all the data relating to all of the service users and their profiles. Therefore, it was found that such filtering would infringe Article 8 of the Charter.[113]

36 However, under the recent Poland, YouTube/Cyando and Glawischnig cases, neither AGs nor the CJEU conducted any balancing test for this specific fundamental right even if both cases discussed injunctions requiring online intermediaries to monitor all information of all users. In fact, none of the parties to these cases have briefed the courts about privacy and data protection concerns. Perhaps, such claims would be a weak defence for YouTube and Facebook who have been dealing with privacy and data protection claims and investigations for their use of users' personal data for targeting practices.[114] However, given that both cases were preliminary rulings for the interpretation of EU law, i.e. Articles 14 and 15 of the ECD, the CJEU would be expected to consider such interpretations in light of fundamental rights and freedoms safeguarded under the Charter.[115] Therefore, it can be argued that the CJEU may accept the processing of users' personal data for filtering measures as legitimate given that all these major hosting providers have already adopted EU data protection standards into their data processing activities within their services. Perhaps, it should be discussed to what extend any automated proactive measure would comply with the requirement of GDPR[116] since some scholars have already raised their concerns over the potential violation of the automated decision-making requirements under Article 22 of the GDPR due to the opaqueness of the algorithms.[117] Due to its limited scope, this article assumes that these concerns can be balanced with the need to prevent online abuses and further, the implementation of automated filtering measures by online intermediaries will be supported by granting users the right to obtain human intervention as required by Article 22 of the GDPR.

2. Problem with Balancing in the Interpretation of General Monitoring

37 Before moving to the conclusion, it is important to point out the underlying problem with the balancing exercise of the CJEU and the ECtHR: interpreting the scope of general monitoring that compromises the very essence of freedom of expression and information and right to privacy of internet users. Although balancing is used by European courts as one of the standard ways through which to determine the outcome of a case where two fundamental rights conflict with each other, weighing two individual-centric, higher rights in a hypothetical scale as a way of human or fundamental rights adjudication has been

111 Keller (n 52); C Angelopoulos and others, 'Study of Fundamental Rights Limitations for Online Enforcement through Self-Regulation' (IViR 2015) <https://dare.uva.nl/search?identifier=7317bf21-e50c-4fea-b882-3d819e0da93a> accessed 6 August 2021.

112 *L'Oréal SA and Others v eBay International AG and Others* (n 10) para 142.

113 *SABAM v Netlog NV* (n 15) paras 48 and 49; The CJEU determined that the collection of IP addresses of internet users by internet access provider would impair user's right to protect personal data, *Scarlet Extended v SABAM* (n 14) para 51.

114 Keller (n 52).

115 *Scarlet Extended v SABAM* (n 14) para 39; Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB and Watson and Others* [2016] ECLI:EU:C:2016:970 para 91 et seq.

116 Regulation (EU) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

117 Christoph Schmon, 'Copyright Filters Are On a Collision Course With EU Data Privacy Rules' (*Electronic Frontier Foundation*, 3 March 2020) <https://www.eff.org/deeplinks/2020/02/upload-filters-are-odds-gdpr> accessed 23 August 2021; Sophie Stalla-Bourdillon, 'Data Protection and Copyright: Could Art. 29 WP Guidance on Automated Decision-Making "Help" with Filters?' (*Peep Beep!*, 30 October 2017) <https://peepbeep.wordpress.com/2017/10/30/data-protection-law-and-copyright-could-art-29-wp-guidance-on-automated-decision-making-help-with-filters/> accessed 23 August 2021; Reda, Selinger and Servatius (n 38).

criticised.[118]Accordingly, the main criticism is that while qualified fundamental rights, such as the right to property, freedom of expression, the right to privacy, precisely aim to act as a barrier for individuals against state interferences which is often supported by or based on majority's view in a democratic society, the identification of interests, assigning commensurable values to those interests on the case by case basis and ultimately to "deciding which interest yields the net benefit" under the test of *balancing* contradicts with the core rationale of the fundamental right concept and consequently constrain themselves to a test of utilitarianism.[119]

38 Furthermore, the necessity test stipulated under Article 52 of the Charter and under Articles 8 and 11 of the Convention allowing limitations on the exercise of the fundamental freedom and rights only if it is necessary in a democratic society in accordance with the principle of proportionality which requires the intensity of the limitation not to be excessive in relation to the protection of the rights and freedoms of others is also accepted as a type of balancing exercise. Because it naturally leads to balancing of interests arising from these competing fundamental rights.[120] Eventually, due to the balancing approach, the courts might no longer seek to determine what is right or wrong in the dispute but, instead, try to investigate which fundamental right yielding net interest for the society concerned in relation to values and priorities upheld at the time. In other words, the balancing approach erodes the very essence and distinctive meaning of fundamental rights by "transforming them into something seemingly quantifiable".[121]

39 Through exploring the CJEU and ECtHR case law, Part 1 presents how general monitoring obligations lead to the clash between two opposing sides: in one corner freedom of expression, the right to privacy and protection of personal data, and the freedom to conduct a business while in the other, the right to privacy in a defamation context and right to property sit. Regarding the methodology, the two courts followed a very similar balancing method. They assess the alleged interference, whether it is provided by law, the existence of a legitimate aim or public interest objective, and, finally, examine necessity. In order to determine what is necessary, both the courts reduce conflicts between two fundamental rights, e.g., freedom of expression and the right to privacy or the right to property to utilitarian comparisons of relative weights or interests on the case by case basis and thus ignores the justification-protective function of rights.[122] Particularly, the defamation cases, such as Delfi, Tamiz, Phil and Glawischnig, show that it is up to the courts to decide what the context-specific interests of freedom of expression and right to privacy are, and consequently what are the limits of these fundamental rights in each case. Depending on the nature of the defamatory content and the size or reach of the online intermediary, the limitations on the exercise of right to receive information changes. Similar problems can be observed in the CJEU rulings in the Youtube/Cyando and Poland v Parliament/Council cases. In both cases, proportionality of the monitoring obligation is assessed based on, among others, the provision of *sufficiently substantiated* information regarding the infringement to the online intermediary.[123] However, the vagueness of sufficient information again led to the arbitrary scope of restrictions. Unfortunately, these cannot be coherent with human rights because the deep values and considerations of these rights are seen as fundamental to human life and therefore, they provide minimum rules and obligations regardless of the context they arise or of their status in the community.[124]

40 Moreover, even if the balancing exercise is justified, almost all the recent rulings seem to overlook the interests or weights of right to privacy and protection of personal data of internet users on this hypnotical scale. Permanent blanket monitoring of all online content and the possibility of false positive results of automated filtering systems, which is subject to the review of moderators who are not targeted by the content generator at the first place is indeed limiting on the right to privacy.

118 Jürgen Habermas, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* (William Rehg tr, MIT Press 1996); Basak Cali, 'Balancing Human Rights? Methodological Problems with Weights, Scales and Proportions' (2 January 2007) <https://papers.ssrn.com/abstract=2406348> accessed 6 July 2022; Stavros Tsakyrakis, 'Proportionality: An Assault on Human Rights?' (2009) 7 International Journal of Constitutional Law 468.

119 Cali (n 118); B van der Sloot, 'The Practical and Theoretical Problems with "Balancing": Delfi , Coty and the Redundancy of the Human Rights Framework' (2016) 23 Maastricht Journal of European and Comparative Law <https://dare.uva.nl/search?identifier=eb7afd99-1e35-4000-a0f4-ece8178e0ab3> accessed 6 July 2022.

120 Tsakyrakis (n 118); Olivier De Schutter and Françoise Tulkens, 'The European Court of Human Rights as a Pragmatic Institution' (6 June 2014) <https://papers.ssrn.com/abstract=2446909> accessed 6 July 2022.

121 Tsakyrakis (n 118).

122 ibid.

123 *Republic of Poland v. European Parliament and Council of the European Union* (n 56) para 91.

124 Cali (n 118).

IV. Interim Conclusion

41 This article shows that, at the beginning of the last decade, the CJEU adopted a broad interpretation of the concept of *general monitoring*. Accordingly, the imposition of any obligation requiring an online intermediary to monitor all information of all service users to filter infringements falls within the scope of the prohibition as it constitutes an excessive burden on the fundamental rights of online intermediaries as well as of internet users.[125] However, in the recent cases, the CJEU has recognised the difficulties for the targeting specific infringement from particular users due to fast-paced information flow of the internet realm, and acknowledged the fact that any preventive measure against illegal content cannot be effective without prior monitoring of all information flowing through the service.[126]

42 Perhaps, this shift from banning monitoring of all information to allowing the same practices for specific infringements can be explained by assessing the validity of the reasons behind the adaptation of the prohibition on the general monitoring obligation in the ECD at the beginning of this millennium.[127] Given the advancement in technology and the rapid economic growth of online intermediaries in recent years, the reasons for the lack of technical capacity and the desire not to deter a developing industry seem to have lost their validity in the eyes of the CJEU. Furthermore, the risk of creating actual knowledge and awareness by monitoring all the content including illegal but not notified ones has also been refused by the CJEU in the YouTube/Cyando case.[128] On the other hand, the risk of over-blocking and the unfairness of imposing obligation upon those mere intermediaries seem to be only valid reasons behind the CJEU's interpretation of Article 15(1) of the ECD. In relation to these concerns, both the European Courts seem to limit the scope of proactive measures against manifestly illegal content that would not require the online intermediary to conduct any legal assessment and only allow its imposition on financially and technically resourceful intermediaries that have influence over the curation of content instead of merely hosting them.[129] Lastly, in any circumstance, intermediaries must implement effective redress mechanisms and safeguards for legitimate personal data processing for internet users.[130]

43 Overall, as per the CJEU's case-law, the permissible monitoring obligations must: (i) be targeted to online content[131] which has been previously identified as illegal by a court[132] or which is manifestly illegal for a reasonable person[133], (ii) not require an additional independent legal assessment to identify,[134] (iii) be effective[135], reasonable[136] and propriate in accordance with the technical, operational and financial capabilities of the intermediary,[137] and with the impact of illegal content[138], for instance anyone of the GAFAM platforms[139], (iv) be carried out on the legitimate basis for the processing of personal data[140], and (v) be supplemented with an appropriate redress mechanism granted to internet users[141].

125 *L'Oréal SA and Others v eBay International AG and Others* (n 17); *Scarlet Extended v SABAM* (n 21); *SABAM v Netlog NV* (n 22); *McFadden v Sony Music* (n 28).; For the explanation of the related judgements, please see Section C, p 18 et seq.

126 *Eva Glawischnig-Piesczek* (n 24) 36; *Peterson/Elsevier v Youtube/Cyando*, Opinion of the AG Saugmandsgaard ØE (55) 221; *Peterson/Elsevier v Youtube/Cyando* (33); Republic of Poland v. European Parliament and Council of the European Union (n 56).

127 For the detailed explanation, please see Chapter B, Section II, p 5 et seq.

128 *Peterson/Elsevier v Youtube/Cyando* (33), para 109.

129 Reda, Selinger and Servatius (n 38).

130 *Republic of Poland v. European Parliament and Council of the European Union* (n 56) para 94.

131 *Delfi AS v. Estonia* (n 79); *Eva Glawischnig-Piesczek* (n 24); *Peterson/Elsevier v Youtube/Cyando* (33).

132 Reda, Selinger and Servatius (n 38); Frosio and Mendis (n 94).

133 Opinion of the AG Saugmandsgaard ØE in case C-401/19 (n 60).

134 Peterson/Elsevier v Youtube/Cyando (33); *Eva Glawischnig-Piesczek* (n 24).

135 *L'Oréal SA and Others v eBay International AG and Others* (n 17) para 136,141; *Eva Glawischnig-Piesczek* (n 24) para 46; *UPC Telekabel Wien GmbH v Constantin Film* (n 41) para 64

136 *L'Oréal SA and Others v eBay International AG and Others* (n 17) para 141,144; *UPC Telekabel Wien GmbH v Constantin Film* (n 41) paras 53,59.

137 *L'Oréal SA and Others v eBay International AG and Others* (n 17) para 141; *UPC Telekabel Wien GmbH v Constantin Film* (n 41), *Peterson/Elsevier v Youtube/Cyando*, Opinion of AG Saugmandsgaard ØE (42).

138 Delfi AS v Estonia 113, 115, 117, 128 and 145.

139 GAFAM is a common abbreviation used to refer to big tech giants, Google, Amazon, Facebook, Apple and Microsoft.

140 *SABAM v Netlog NV* (n 62); *Scarlet Extended v SABAM* (n 62).

141 *UPC Telekabel Wien GmbH v Constantin Film* (n 41)

44 It must be noted that Senftleben and Angelopoulos (2021) refused this general conclusion as they believe that the standards for the prohibition on general monitoring must be "specific in respect of both the protected subject matter and potential infringers".[142] First, they argued that the Glawischnig-Piesczek judgement is incompatible with the CJEU's rulings in the SABAM, McFadden, and L'Oréal cases because the infringements in intellectual property law depend not only on the specific use of work but also on the identity of the specific group of users.[143] Furthermore, Senftleben and Angelopoulos (2021) also pointed out that while it is often sufficient to identify the protected work that is fixed after the first publication in copyright issues, defamation cases, by contrast, depend on the nature of uploaded content and the use of specific defamatory elements in specific contexts.[144] Due to these substantial differences, the standards of general monitoring will be shaped based on "the nature and scope of the legal position, in respect of which the imposition of duties of care, including the introduction of content moderation duties, is requested".[145] While this is a plausible argument, considering the horizontal nature of the ECD, and both AG Saugmandsgaard-ØE's interpretation of manifestly illegal content in Poland v Parliament and Council case with the explicit reference to AG Spunzar's interpretation in Glawischnig-Piesczek case,[146] this article accepts the horizontal effect of the CJEU's interpretation of the scope of *specific monitoring* in line with Reda et al (2020), and Van Eecke (2011), and it argues that monitoring obligation for specific infringement is permissible regardless of the nature of infringement as long as the identification of illegal content can be carried out without any legal assessment of intermediaries and the effective redress mechanisms are implemented.[147]

C. Interplay Between the Prohibition on General Monitoring Obligation and the Evolving EU Legislations.

45 This chapter will analyse the role of general monitoring within the new online intermediary liability regime introduced under the new EU legislations by comparing the implementation of the prohibition with the CJEU's interpretation. The aim is to reveal the inconsistencies between these legislations and the CJEU's interpretation.

I. Audiovisual Media Services Directive

46 In 2018, the EU amended the AVMSD[148] to introduce new requirements for VSP provider, a recently defined subset of hosting service provider.[149] According to Article 28b, member states must ensure that VSP providers adopt "appropriate, practicable and proportionate" measures to protect minors from online content which may impair their physical, mental or moral development and the general public from the dissemination of content containing hate speech and incitement to violence, provocation to commit terrorist offence, child sexual abuse material and racism and xenophobia.[150] The AVMSD further provides a non-exhaustive list of measures that are deemed appropriate by EU legislators including, among others, the notice and take down systems based on user's reporting[151] but also allow Member States to impose more detailed and stricter measures

142 Christina Angelopoulos and Martin Senftleben, 'An Endless Odyssey? Content Moderation Without General Content Monitoring Obligations' (22 June 2021) <https://papers.ssrn.com/abstract=3871916> accessed 9 July 2022.

143 Martin Senftleben and Christina 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' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3717022 <https://papers.ssrn.com/abstract=3717022> accessed 21 May 2021."plainCitation":"Martin Senftleben and Christina 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' (Social Science Research Network 2020

144 Angelopoulos and Senftleben (n 142).

145 ibid.

146 *Peterson/Elsevier v Youtube/Cyando*, Opinion of AG Saugmandsgaard ØE (42), para 221; Opinion of the AG Saugmandsgaard ØE in case C-401/19 (n 60) para 113.

147 Reda, Selinger and Servatius (n 38) 19,20; Patrick Van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach' (2011) 48 Common Market Law Review 1487 <http://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/48.5/COLA2011058> accessed 23 August 2021.

148 The AVMSD.

149 For detailed definition please see Chapter IV, Section A, Part i, p 31 et seq.

150 The AVMSD Article 28b(1),(2).

151 Ibid Art 28b(3).

on VSPs.[152] However, these measures shall not lead to ex-ante control measures or upload-filtering of content, which do not comply with Article 15 ECD.[153]

47 It becomes evident that the EU lawmakers consider the balance test requirement for the determination of appropriate, practicable and proportionate measures in line with the CJEU's case-law.[154] But, it is not clear as to what measures could be stricter than a notice and takedown procedure in the context of the available technology[155] but do not constitute ex-ante content moderation measures, which are clearly considered a violation of Article 15 of the ECD. Moreover, this prohibition of *ex-ante control measures* and *upload-filters* fails to reconcile the YouTube/Cynado, Glawishking and Poland v Parliament/Council rulings as well as the ECtHR's case-law, which allow the imposition of monitoring obligation to prevent *manifestly* illegal content.[156]

II. Regulation on Preventing Dissemination of Terrorist Content Online

48 The Regulation on Preventing Dissemination of Terrorist Content Online enacted in May 2021 imposes obligations on hosting service providers to remove terrorist content within an hour upon receipt of a notification from a competent authority.[157] Hosting service providers must take specific measures to protect their services from being misused for the dissemination of terrorist content if the competent authority finds the service is exposed to terrorist content on basis of certain factors, such as having received two or more removal orders from a competent authority within the past twelve (12) months. In line with the settled balancing test of the CJEU, the Regulation also grants freedom to hosting service providers on their choice of specific measures on condition that these measures must be effective in mitigating the risk, proportionate with the technical, financial, and operational capabilities, the number of users of the hosting service provider and the amount of content they provide.[158] The competent authorities also have power to require additional specific measures if they find the hosting service provider's measures are insufficient to address the risks.[159] Nevertheless, the imposition of any requirement leading a general obligation to monitor or actively seek facts or circumstances indicating illegal activity under Article 15(1) ECD or to use of automated tools by hosting providers are prohibited.[160]

49 Once again, the prohibition on general monitoring appears as the borderline for statutory specific measures. However, the whole system established under the Regulation including the obligation to remove notified terrorist content and to take specific measures for the protection of the service, seems to give no other option to hosting providers

152 Ibid Art 28b(6).

153 Ibid Art 28b(3),(6).

154 Commission Staff Working of 25 May 2016, Impact Assessment of AVMSD Proposal, SWD(2016) 168.

155 In the automated content moderation, two techniques are mainly adopted by VSPs, i.e. the matching and classification technique. In the matching, filtering system automatically review newly uploaded audio-visual content against a large table of existing fingerprints of previously removed harmful content which is generated based on either whole audio-visual file or specific elements or features of such content such as certain colours, corners in images, hertz-frequency of sound etc. For instance, YouTube's CSAI Match, Microsoft PhotoID and Facebook's PDQ and TMK+PDQF are examples of the filtering systems based on this technique systems and used for the detection of child sexual exploitation, terrorist propaganda, and graphic violence. The classification technique based on Machine Learning or Deep Neural Network solutions and are used for object detection, scene understanding, and semantic segmentation, or advanced video understanding. Object detection and semantic segmentation can identify certain objects such as weapons, faces, body parts, and text within images and their location within an image through processing regions of an image or video and associating it with predefined features of harmful content such as nudity, violence, hate speech etc. For more information, please see; Analisa Tamayo Keef and Lior Ben-Kereth, 'Introducing Rights Manager' (*Facebook for media*, 12 April 2016) <https://perma.cc/YB5H-BEM5> accessed 23 June 2021; Tony Wang, 'Recognizing Firearms from Images and Videos in Real-Time with Deep Learning and Computer Vision' [2019] *Medium* <https://medium.com/@tont/recognizing-firearms-from-images-and-videos-in-real-time-with-deep-learning-and-computer-vision-661498f45278> accessed 23 June 2021; 'Use of AI in Online Content Moderation' (Cambrige Consultants 2019) <https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/online-content-moderation>; Gorwa, Binns and Katzenbach (n 65).

156 For legal analysis of these case-laws, please see Chapter II, Section B, C, p 9 et seq.

157 As per Article 12 of the Regulation on Preventing Dissemination of Terrorist Content Online, competent authorities will be designated by each member states.

158 Ibid Art5(1), Recital 22.

159 Ibid Art 6.

160 Ibid Art 8.

but to take certain proactive measures in practice. First, as the obligation to take specific measures is triggered by the receipt of more than two removal orders, without any preventive measures, the previously removed terrorist content can be easily re-uploaded and cause the competent authorities to issue additional third removal order which eventually trigger the requirement to take so-called specific measures. Moreover, Article 5(2)(a) classifies "appropriate technical and operational measures or capacities, such as appropriate staffing or technical means to identify and expeditiously remove or disable access to terrorist content" as a permissible specific measure which clearly requires *de facto* monitoring of uploaded content in order to identify terrorist content. Given that Article 7(3)(b) also requires providers to publish information about measures taken to address the *reappearance* of previously removed content annually, it becomes apparent that hosting providers are expected to take preventive measure at some degree, for instance against the pre-identified terrorist content.[161]

50 To a certain extent, the suspension of users or accounts that are identified as terrorist content uploader can be considered a preventive measure. However, the privacy concerns over the loss of online anonymity[162] and the availability of technologies that provide anonymity[163] would hamper the effectiveness of these suspensions. Therefore, considering the requirement for specific measures to be *effective, appropriate and proportionate* in accordance with a hosting provider's size, technical and economic capacity, and the number of its users,[164] it becomes evident that major hosting service providers enabling access to user content in large scales do not have any other option to effectively mitigate the dissemination of terrorist content but to implement the filtering measure for pre-identified terrorist content. Indeed, this understanding would comply not only with both the EU legislators' recent statements concerning the proactive measures against manifestly illegal content[165] but also with the CJEU's interpretation of Article 15(1) ECD.[166] In fact, all necessary safeguards for fundamental rights stipulated by the CJEU have already been considered under the Terrorist Content Regulation such as the proportionality test, human oversight, and verification in the use of automated tools against over-blocking and the introduction of complaint and redress mechanisms.[167] However, if the CJEU's interpretation is accepted and the hosting providers can be forced to take *technical and operational measures* to identify and expeditiously remove pre-identified terrorist content under Article 5(2)(a), this Regulation would be incompatible with the prohibition of ex-ante control measures as provided for under the AVMSD.

III. The Directive on Copyright in the Digital Single Market

51 The obligations stipulated under Article 17(4) of the Copyright Directive were the subject of one of the most influential CJEU rulings, Poland v Parliament/Council. According to Article 17(4), online content-sharing service providers ("OCSSP")[168] which have not obtained an authorization from the rightholders must demonstrate that they have: (i) made best efforts to ensure the unavailability of specific copyright-protected works for which the relevant rightholders must have provided the OCSSP with the relevant and necessary information and (ii) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to remove the content infringing the notified works and made best offers to prevent their future uploads.[169] The assessment of "best efforts" is made in accordance with "high industry standards of professional diligence" and the principle of proportionality with regard to the number of elements such as the type,

161 Aleksandra Kuczerawy, 'Proposed Regulation on Preventing the Dissemination of Terrorist Content Online' (For Center for Democracy and Technology 2018) <https://cdt.org/insights/research-paper-from-leuven-university-proposed-regulation-on-preventing-the-dissemination-of-terrorist-content-online/> accessed 17 August 2021.

162 Rachel Melis, 'Anonymity Versus Privacy in a Control Society' (2019) 2 Journal of Critical Library and Information Studies <https://journals.litwinbooks.com/index.php/jclis/article/view/75> accessed 17 August 2021.

163 Thais Sardá and others, 'Understanding Online Anonymity' (2019) 41 Media, Culture & Society 557.

164 Regulation on Preventing Dissemination of Terrorist Content Online, Recital 24.

165 European Parliament, 'Resolution of 20 October 2020 on the Digital Services Act and fundamental rights issues posed (2020) 0274, para 27; Commission, Recommendation on measures to effectively tackle illegal content online.

166 Please see Chapter II, Section D 'Interim Conclusion', p 22 et seq.

167 Terrorist Content Regulation Art 5, 10.

168 The Directive on Copyright in the Digital Single Market, Article 2(6) defines online content-sharing service provider as "*a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes*".

169 Ibid Art 17(4).

the audience and the size of the service, the evolving state of the art to avoid the availability of different types of content and the cost of such means for the services.[170] In fact, Article 17(6) exempts new OCSSPs from the "best effort" requirement that have been active in the EU for less than 3 years, have less than 5 million monthly unique visitors and have an annual turnover of less than 10 million euros. Lastly, Article 17(8) explicitly states that the application of best effort requirements under Article 17 shall not lead to any general monitoring obligation.[171]

52 The EC's Guidance on Article 17 recognises the content recognition technologies as a method "commonly used today to manage the use of copyright protected content, at least by the major online content-sharing service providers and as regards certain types of content" and note that these technologies can be considered as the market standards to filter and block *manifestly infringing* content for large OSSPs.[172] In the Poland v Parliament/Council case, the CJEU confirmed this position by explicitly announcing that the requirement for use of automated recognition and filtering technologies under the best effort obligations, do not amount to general monitoring obligations that could hamper the providers.[173] Basically, both the EC and CJEU agreed that upload filters can be compatible with the prohibition as long as the scope of filtering measures is limited to specific infringement identified by courts or rightholders and which is specific enough to be detected by automated tools.[174] In addition, they noted that certain safeguards must be implemented for fundamental rights in particularly freedom of expression and right to remedy.[175]

170 Ibid Art 17(5), Recital 65.

171 Ibid Art 17(8).

172 Commission 'Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market' COM (2021) 288 Final, ('Guidance on Article 17') pages 12,22.

173 *Republic of Poland v. European Parliament and Council of the European Union* (n 56).

174 Guidance on Article 17, p 16; Case C-401/19, *Republic of Poland v European Parliament and Council of the European Union* [2019], Opinion of AG Saugmandsgaard ØE paras 200-201.

175 Guidance on Article 17, p. 22; The Directive on Copyright in the Digital Single Market Article 17(9), Recital 70; *Republic of Poland v European Parliament and Council of the European Union* [2019], Opinion of AG Saugmandsgaard ØE 98 et seq.

D. The Implementation of General Monitoring Prohibition on Video-Sharing Platforms

53 This last chapter elaborates how this discrepancy concerning the notion of general monitoring under the EU legislations will affect VSPs in practice. However, in order to conduct such legal analysis, first an explanation needs to be made of why VSPs fall within the scope of these legislations.

I. Understanding Video-Sharing Platforms

1. Definition

54 VSP services are defined under Article 1(aa) of the AVMSD. Accordingly, any information society service satisfying the following three conditions is VSP service: (i) the principal purpose of the service or of a dissociable section thereof, or an essential functionality of the service is devoted to providing programmes, user-generated videos ("UGV"), created and uploaded by a service user, or both, to the general public, for which the service provider does not have editorial responsibility, in order to inform, entertain or educate; (ii) the service is made available by means of electronic communication networks and (iii) the organisation of these content is determined by the provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing.[176]

55 The assessment of whether video-sharing is "principal purpose" of the service or "dissociable section" thereof simply refers to hosting service providers that do not have any features or services other than video sharing, or the home page of which is devoted to shared videos or have a section listed in the navigation of a website or accessible from a link or icon on an app home screen that provides video-sharing or upload.[177] Considering these parameters, YouTube, TikTok, and all adult VSPs become VSP providers due to principal purpose of services, while

176 The AVMSD, Art 1(aa).

177 Yi Shen Chan, Sam Wood and Stephen Adshead, 'Understanding Video-Sharing Platforms Under UK Jurisdiction' (Plum Consulting 2019) <https://plumconsulting.co.uk/understanding-video-sharing-platforms-under-uk-jurisdiction/> accessed 21 May 2021.; EU Guidelines on the practical application of the essential functionality criterion of the definition of a 'video-sharing platform service' under the Audiovisual Media Services Directive (n 138).

Vimeo[178], Instagram's IGTV[179] which is mainly and Facebook's Watch Section[180] can be identified as VSPs whose dissociable section of principal service is video sharing.

56 If this assessment cannot be made, then it should be assessed whether the provision of UGV or programmes is an "essential functionality" of the service of an online intermediary. As per Recital 5 of the Directive 2018/1808, a service could have the "essential functionality" of the provision of videos if "the audiovisual content is not merely ancillary to, or does not constitute a minor part of" the activities of that service.[181] For the essential functionality test, the EC has determined four main indicators under its Guidelines.[182] Although these guidelines are not legally binding, and do not provide uniformity of interpretation, because of their relevance, this article takes into account for the determination of the scope of the AVMSD.

57 As per the Guidelines, the essential functionality requires that audiovisual content has discretely core value on the main service. This should focus more on the architecture and operation method of the online intermediary to determine whether the video-sharing feature constitutes a stand-alone function on the service.[183] Secondly, the quantitative and qualitative relevance of audiovisual content for the service such as the amount, use and reach of audiovisual content needs to be reviewed collectively.[184] Third, whether the online platform gains revenue through its video-sharing features by example ads placement, pay-to-access system, or processing of users data for various marketing/ commercial purposes in exchange of views.[185] Lastly, whether the service promotes the user's engagement with shared video is assessed.[186] These indicators must be considered under an overall analysis of the service and the absence of one or more of them does not automatically exclude the service from being a VSP. The AVMSD applies to the intermediary if the results of a sufficient number of indicators support the conclusion that the provision of audiovisual content is not merely ancillary or a minor part of, the activities of that intermediary's service. In line with this conclusion, Snapchat[187], Reddit[188] and Twitter[189] can be identified as VSP providers as the video-sharing functionality of their platforms has become an essential function of their social networking services.[190]

58 The last important element is the absence of editorial responsibility. It separates VSPs providers from being "media service providers" who have legal obligation to comply with certain requirements in relation to commercial communication, audiovisual advertising, sponsorship and product placement under the AVMSD. According to Article 1(1)(c), editorial responsibility refers to the exercise of effective control over both the selection of the programmes and the organisation either in a chronological schedule or in a catalogue.[191] Given that the definition of VSP service acknowledges the organisational control over the content, the distinctive factor becomes

178 Vimeo's main service is pivoted into software provision for video production and storage and does not monetise video-sharing activities.

179 Instagram was first launched as photo-sharing social network, however in recent years, it embedded video-sharing function on its app and website. Although it's principle purpose of service might be considered as the provision of UGV to the general public, its initial photo-sharing function still constitutes as principle element of the service.

180 Chan, Wood and Adshead (n 164).

181 The AVMSD Recital 5.

182 Guidelines on the practical application of the essential functionality criterion of the definition of a 'video-sharing platform service', (n 156).

183 Ibid p 6.

184 Ibid p 7.

185 Ibid pp 7-8.

186 Ibid pp 8-9.

187 Tiffany Peón, 'A Guide to Snapchat for People Who Don't Get Snapchat' *The New York Times* (7 February 2018) <https://www.nytimes.com/2018/02/07/smarter-living/snapchat-guide.html> accessed 22 August 2021. While its principal purpose of the service is to provide a camera and messaging application, the video-sharing function has become more dominant in recent years.

188 Christian Stafford, 'What Is Reddit? - Definition from WhatIs.Com' <https://searchcio.techtarget.com/definition/Reddit> accessed 22 August 2021.

189 'How to Go Live on Twitter with Twitter Live Stream Feeds' <https://help.twitter.com/en/using-twitter/twitter-live> accessed 22 August 2021; 'How to Share and Watch Videos on Twitter' <https://help.twitter.com/en/using-twitter/twitter-videos> accessed 22 August 2021.

190 Joan Barata, 'Regulating Content Moderation in Europe beyond the AVMSD' (*Media@LSE*, 25 February 2020) <https://blogs.lse.ac.uk/medialse/2020/02/25/regulating-content-moderation-in-europe-beyond-the-avmsd/> accessed 15 June 2021.

191 AVSM Directive Art 1(c).

the ability to decide and select which content will be available on the service. Therefore, this sole power over the selection of the content distinguishes VSP providers from other audio-visual content providers such as publishers whose website includes videos regarding news or subscription-based video-on-demand services, or broadcasters providing content online on their website as well as online platforms.

2. Legal Framework

59 The previous commentary on the definition of VSP service under Article 1(aa) AVMSD reveals that nearly all of today's popular social networks fall within the scope of Article 28b of AVMSD.[192] Furthermore, the UGV hosted by VSPs are broadly defined as an individual set of moving images with or without sound created by an internet user and uploaded to a VSP by that user or any other user which could cover most of today's online content.[193] As VSPs host their user's information in form of, audiovisual content and transmit it to other users through electronic means, without actively selecting the content, they become a subset of hosting service providers under the ECD.[194] Therefore, as a result of being a hosting service provider, VSPs also fall within the scope of the Terrorist Content Regulation.[195]

60 Moreover, the OCSSP definition under Article 2(6) the Copyright Directive, with the emphasis on the function to store and give the public access to large amount of copyright-protected works which are organised by the OCSSP for profit-making purposes and the thresholds set forth by Article 17[196] are clearly designed to include major VSPs.[197] Overall, it can be concluded that the commercially large-scale VSPs are obliged to implement necessary measures against certain types of illegal content online in accordance with the AVMSD, the Terrorist Content and the Copyright Directive.

II. To What Extend the Prohibition of General Monitoring Should Be Applied on Video-Sharing Platforms under the EU Legislations.

61 It is evident that there is a lack of a uniform application of general monitoring prohibition within the EU intermediary liability regime. Whereas the AVMSD qualifies ex-ante control measures and upload-filters as prohibited general monitoring regardless of the nature of the content and the Terrorist Content Regulation prohibits obligation to use automated tools against terrorist content[198], the Copyright Directive, in line with the CJEU's interpretation, obliges VSPs to implement automated filtering measures against specific copyright infringements. In practice, these different approaches regarding content moderation measures might cause VSPs which host both video, image and textual content like Instagram or Twitter to face difficulties depending on whether manifestly illegal potential content is posted by video, or within a still image or as a written article.[199]

62 Firstly, while both the AVMSD and the Terrorist Content Regulation aim to tackle with the dissemination of the terrorist content, the required measures differ significantly under each legislation. According to AVMSD, VSPs cannot be forced to implement upload-filters, but on the other hand, the Terrorist Content Regulation expects them to prevent the recurrence of previously removed terrorist content. This

192 Barata (n 177); Francisco Javier Cabrera Blázquez and others, *The Legal Framework for Video-Sharing Platforms* (European Audiovisual Observatory 2018).

193 Ibid Art 1(b)(ba), Directive 2018/1808, Recital 6.

194 Jan Oster, *European and International Media Law* (Cambridge University Press 2016) <https://www.cambridge.org/core/books/european-and-international-media-law/11DB5E88696AE095F61FE885E190B762>.; The E-Commerce Directive Recital 18; Joined Cases C-682/18 and C-683/18, Peterson/Elsevier v Youtube/Cyando (n 54) para 117, the CJEU acknowledge that activities of VSP providers fall within the scope of Article 14 of the ECD.

195 The Terrorist Content Regulation, Article 1.

196 For the detailed explanation of these thresholds, please see Chapter III, Section C, p 29 et seq.

197 João Quintais, 'The New Copyright in the Digital Single Market Directive: A Critical Look' (2019) 2020 European Intellectual Property Review <https://papers.ssrn.com/abstract=3424770> accessed 23 August 2021; Karina Grisse, 'After the Storm—Examining the Final Version of Article 17 of the New Directive (EU) 2019/790' (2019) 14 Journal of Intellectual Property Law & Practice 887; Christophe Geiger and Bernd Justin Jütte, 'Towards a Virtuous Legal Framework for Content Moderation by Digital Platforms in the EU? The Commission's Guidance on Article 17 CDSM Directive in the Light of the YouTube/Cyando Judgement and the AG's Opinion in C-401/19' <https://papers.ssrn.com/abstract=3889049> accessed 10 August 2021.

198 This is the result of the interpretation made under this paper, please see Chapter III, Section B, p 26 et seq.

199 This was the issue in the Case C-18/18, Eva Glawischnig-Piesczek v Facebook (n 48).

means VSPs cannot be required to take measures to "identify and expeditiously remove" pre-identified terrorist content under Article 5(2)(a) the Terrorist Content Regulation, as it contradicts with the AVMSD. However, without implementing ex-ante monitoring to tackle previously removed terrorist content and by solely relying on reactive measures, there will be a loop of constant uploads and one-hour removals of the same terrorist content.

63 If the prohibition of general monitoring under the Terrorist Content Regulation is read in compliance with the AVMSD, then the specific measure under Article 5 would not go beyond being the supplementary list to the non-exhaustive list of appropriate measures under Article 28b of the AVMSD. Furthermore, there is nothing to stop national courts from issuing an injunction on VSPs to prevent pre-identified terrorist content on its service. This will eventually lead to VPSs with thousands of daily uploads to implement an automated filtering system to comply with such injunction even if it cannot be required under the Terrorist Content Regulation. Given that the CJEU identified automated recognition and filtering tools as an effective measure against dissemination of illegal content in the Poland v Parliament/Council judgement, the prohibition on requirement for the use of automated tools under the Terrorist Content Regulation perhaps becomes an empty shell in practice at least for large service providers as they do not have any other option but to implement automated systems other than employing thousands of human moderators.

64 Secondly, there is an imbalance between rights and interests under the current legislative framework. The interests at stake for the prevention of reappearance of content containing non-consensual sexual videos, child sexual abuse, provocation to commit a terrorist or extremist offence which are pre-identified by judicial authorities as illegal are considerably higher than the interest of copyright holders protected under Article 17 of the Copyright Directive.[200] In fact, today, the automatic duplicate-detection systems are the most commonly deployed systems to filter out duplicates of known, specific terrorist or child exploitation images, audio, or videos in practice, and they even provide more successful results then human moderators.[201] On the other hand, despite the recent developments in the content recognition technologies, empirical studies show that these systems still perform poorly for the detection of infringements that contain the same, previously notified copyright-protected work.[202] Considering the balance test conducted by both European Courts, it is evident that the monitoring obligations against these manifestly illegal content would constitute a more proportionate limitation on the exercise of the freedom of expression and VPS's freedom to conduct a business. Therefore, the AVMSD's interpretation of general monitoring which covers upload-filters against child sexual abuse and provocation to terrorism and extremism seriously hamper the EU's aim to create a safe digital single market.[203]

65 On the other hand, this article does not disregard the concerns over the risk of excessive restriction of fundamental rights posed by any monitoring obligation requiring an independent assessment of VPSs or national administrative authorities. In addition to risks explained under the case-law review above, as per Balkin (2014), by imposing general monitoring obligation, governments can acquire the power to impose "collateral censorship" on free speech online through the hands of the VSPs.[204] Moreover, it is evident that monitoring of all user information to detect not only manifestly illegal but also other types of illegal content, which require legal assessment, would preclude individuals from sharing and discussing their ideas online and eventually harm their intellectual privacy.[205]

200 Giancarlo Frosio and Christophe Geiger, 'Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime' (2020) Forthcoming European Law Journal <https://papers.ssrn.com/abstract=3747756> accessed 1 August 2021.

201 Olivia Solon, 'Facebook, Twitter, Google and Microsoft Team up to Tackle Extremist Content' *the Guardian* (6 December 2016) <http://www.theguardian.com/technology/2016/dec/05/facebook-twitter-google-microsoft-terrorist-extremist-content> accessed 16 August 2021; Tracy Jan and Elizabeth Dwoskin, 'A White Man Called Her Kids the N-Word. Facebook Stopped Her from Sharing It.' *Washington Post* (31 July 2017) <https://www.washingtonpost.com/business/economy/for-facebook-erasing-hate-speech-proves-a-daunting-challenge/2017/07/31/922d9bc6-6e3b-11e7-9c15-177740635e83_story.html> accessed 16 August 2021. For further information on automated filtering systems which are currently deployed by VSPs, please see fn 128.

202 Joanne E Gray and Nicolas P Suzor, 'Playing with Machines: Using Machine Learning to Understand Automated Copyright Enforcement at Scale' (2020) 7 Big Data & Society 2053951720919963; Daniel Seng, 'Copyrighting Copywrongs: An Empirical Analysis of Errors with Automated Dmca Takedown Notices' (2021) 37 Santa Clara High Technology Law Journal 119.

203 Montagnani (n 7); Ullrich (n 8).

204 Jack M Balkin, 'OLD-SCHOOL/NEW-SCHOOL SPEECH REGULATION' (2014) 127 Harvard Law Review 2296, 2311.

205 Neil Richards, 'A Theory of Intellectual Privacy', *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford Uni-

Unfortunately, it seems like these considerations are overlooked under the balancing exercise of the European human rights adjudicators. Whereas the monitoring obligation should be accepted as a direct interference with the freedom of expression, the right to privacy of internet users and the proportionality test as per Article 52 of the Charter needs to be applied in this context, we have witnessed mere utilitarian comparison of fundamental rights without considering principled hierarchy of interests. As rightly pointed out by van der Sloot (1998), the case law review under Chapter B, Section III of this paper presents minor interests, "such as not being called a rascal or the copyright protection of a commercial business," are promoted to fundamental rights discourse under the balancing exercise.[206] The special protection to certain principles and interests which are deemed essential not only to human life but also to modern day democratic societies, such as the right to receive and impart information on VSPs seems to be forgotten in the interpretation of general monitoring obligations by both the CJEU and the EU legislators.

66 Lastly, imposing specific monitoring obligations against defamatory content might be very problematic in practice. While the copyrighted works can be detected by automatic recognition tools regardless of the format of content, such as video, text, audio, automatic recognition of defamatory content may not always be easily done. For instance, if the defamatory content in Glawischnig-Piesczek case would have been re-uploaded as a video to Facebook where a random person reads the text of the original defamatory content in a different but commonly use language, would this video still qualify as *equivalent content* to original as the message remains essentially unaltered? Or what if this video does not include any audio but just shows series of cardboards where the original messages are written? Or should we expect VSPs to prevent occurrence of such video if it was a part of reporting activities of an amateur journalist?

67 In light of these considerations, it becomes evident that one horizontally applicable prohibition not only creates legal uncertainty for VSPs but also fails to address interests of internet users in the online realm. Therefore, at the current situation, the evolving content/sector-specific EU legislations may include provisions which clearly distinguish the default prohibition on general monitoring obligations from the context-specific measures and which are tailored to address each specific type of illegality in a limited scope and under conditions that overwhelmingly safeguard the interest of individuals in exercising their freedom of expression and right to privacy.[207]

E. Conclusion

68 All in all, this article made three distinctive conclusions. First, by analysing the CJEU's case-law, it notes that the proactive monitoring and filtering obligations targeted to a specific kind of illegality are permitted for, at least, financially and technically resourceful online content hosting and sharing services as long as safeguards for the right to effective remedy and right to protection of personal data and privacy are guaranteed.[208] This exercise reveals that the main concerns behind the prohibition are the negative impacts arising from the imposition of obligation on online intermediaries to carry out an independent assessment of the nature of content and being liable of this assessment. This will cause an excessive burden on online intermediaries which are, to a certain extent, still considered as being passive players or *mere conduits* of content stored or transmitted through their services by third parties and result them to over-remove the legitimate user content. However, the CJEU's adaptation of balancing exercise is found overlooking the special protections for individual and communal interests in the right to privacy and freedom of expression and information in an online environment. Particularly, the possible chilling effect on internet users arising from ex-ante monitoring practices seem not to be assessed in detail by the CJEU.

69 Secondly, under the recent EU legislations, there is a legal uncertainty on which types of obligations to monitor online content in order to prevent the dissemination of illegal content, are prohibited. This is the result of the conflicting interpretations on the scope of the prohibited general monitoring by the EU legislators and the CJEU. Thirdly, it has been noted that the broad definition of VSPs leads almost all the major online intermediaries to legal uncertainty regarding their content moderation practices and thus turning the Article 15(1) of the ECD in an empty shell. As this causes a detrimental impact on the rule of law, this article acknowledges the need for a clear distinction for VSPs between vertically applicable measures arising content or sector specific regulations and the prohibition on blanket monitoring obligations.

70 As for the future, this article foresees the potential

versity Press, Incorporated 2015) <http://ebookcentral.proquest.com/lib/ed/detail.action?docID=1910138> accessed 12 April 2021.

206 van der Sloot (n 119).

207 Sartor and Loreggia (n 9).

208 Please see Chapter II, Section D, p 22 et seq.

violations of the fundamental European values by monitoring obligations and thus questions the need for *ex-ante monitoring* to prevent occurrence of illegal content or illegal activities online. The 21st century world is the dynamic convergence and symbiosis of both the physical and cyber worlds where almost every day digital and physical actions become more intertwined. As the line between real and digital is blurring day by day, perhaps, it is time to reevaluate our legal methodology to regulate this new world. Imposing *ex-ante* monitoring obligation on VSPs for all the information hosted on their services to prevent the occurrence of violations summons the dystopic future depicted in the movie *The Minority Report* in which the police use technology to catch criminals before a crime is committed.[209] As the law does not refuse people from thinking about copying copyrighted works for personal use or having libellous thoughts of another individual, this should also not be the duty for VSPs with respect to online activities of their users. Thus, it is up to us to find an alternative solution that can suppress the impact of online illegal activities without restricting the fundamental rights of individuals.

209 Steven Spielberg, *Minority Report* (Twentieth Century Fox, Dreamworks Pictures, Cruise/Wagner Productions 2002).