Gergely Gosztonyi* – Ewa Galewska** – Andrej Školkay***

Challenges of Monitoring Obligations in the European Union's Digital Services Act

Abstract

The article argues that the Digital Services Act, as part of the EU's broader attempt to regulate intermediary services providers in a constantly growing and challenging technological, social and political environment, does not provide a final and comprehensive solution to the issue. The Digital Services Act appears inconsistent with the previous case law of European supranational judiciary forums regarding the prohibition of general monitoring by intermediary services providers. In fact, it provides the Member States with vaguely worded regulatory exceptions in the event of a ban on general monitoring. However, the Digital Services Act can be seen as a legitimate and necessary attempt to enforce the regulation at the European level through Member States while at the same time giving a unique regulatory position in specific cases to the European Commission or pan-European legal bodies in general. Finally, the Digital Services Act also turns initial enforced self-regulatory attempts to regulate social harms, possibly caused by intermediary services providers, into co-regulation.

Keywords: digital services, Digital Services Act, DSA, monitoring obligations, providers of intermediary services, PIS, E-commerce Directive, ECD

* Gergely Gosztonyi (PhD, Dr. habil) is an Associate Professor at Eötvös Loránd University (ELTE), Faculty of Law, Budapest, Hungary (e-mail: gosztonyi@ajk.elte.hu). His research was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

** Ewa Galewska (PhD, Dr. habil) is a Professor at University of Wrocław, Faculty of Law, Administration and Economics, Wrocław, Poland (e-mail: ewa.galewska@uwr.edu.pl).

*** Andrej Školkay (PhD, Dr. habil) is a Professor at School of Communication and Media, Bratislava, Slovakia (e-mail: askolkay@gmail.com).

I Introduction

In this article, we discuss selected aspects of critical issues and related developments of platforms' general monitoring obligations within the European Union (EU) law and the relevant case law. The idea of this article is not to assess whether measures that lead to general monitoring obligations would be appropriate in the digital EU, for instance, from the perspective of the human rights system. It aims to emphasise that the well-established regime of liability for illegal online content and measures developed and promoted by the EC are inconsistent. It is therefore time to say that a revolution in the field of liability is already happening but also requires a revision of the old regime, and the EU cannot avoid facing this problem.

It should be mentioned first that the Digital Services Act (DSA[1]) uses the term *provider of intermediary services* (PIS) rather than more popular (but arguably less precise as well as more diverse) terms such as *social media* or *online platform* or even the previously used (and sometimes still used) term, *Internet Service Providers* (ISPs). It should also be noted that another term, *information society services,* is also used, namely in the E-commerce Directive (ECD[2]). In short, *intermediary service* means one of the selected and enumerated 'information society services' (see DSA Article 3(g)).

As the core regulation before the DSA was the ECD, we first tackle its regulatory approach in the article. In the last more than twenty years, it turned out that the wording of the directive was not precise enough; international courts, such as the Court of Justice of the European Union (CJEU), tackled the most controversial regulatory issues and helped the legal developments in this area.

We also discuss how monitoring obligations, as a very specific and arguably key aspect of Digital Services regulation, has evolved in the DSA. We emphasise that the established regime of PIS' liability for illegal content online and measures developed and promoted by the European Commission (EC) is inconsistent. It is therefore time to say that a revolution in the field of PIS' liability is already happening but also requires a revision of the old regime, and the EU must tackle this challenge. This overview is, therefore, rather selective. We start with the fundamental idea – the prohibition of general monitoring – then we move our discussion toward the case law of general monitoring in the practice of the CJEU. Next there is a discussion of general monitoring in the EU legislation after the ECD and finally we show how a ban on general monitoring in the DSA is defined and discuss two general exceptions. Furthermore, we discuss some potentially controversial conditions for these exceptions from the ban on general monitoring. We conclude by pointing out a certain

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L178/1.

remaining inconsistency concerning monitoring obligations in the Digital Services Package, specifically in the DSA.

II Prohibition of General Monitoring in the EU

When the Television Without Frontiers Directive (TWFD) was amended in 1997, it was suggested that the new audiovisual regulation should also cover the Internet, but this proposal failed in the European Parliament (EP).[3] As a result, a formal distinction has emerged between traditional media services, where the provider determines the time at which content can be consumed *(push),* and Internet-based services, for which the consumer can choose when *(pull).* This gave rise to the concept of *information society services,* which has become one of the key concepts since the adoption of the ECD in 2000. Information society services 'span a wide range of economic activities which take place on-line' (ECD Recital 2). However, it is evident throughout the careful wording of the directive that it was 'reflecting the policy consensus that the internet should not be brought under existing media regulatory regimes',[4] thus forming a kind of transition between the early Internet legal vacuum and traditional state regulation.[5] For example, in the period between when the Digital Services Package and ECD were adopted, the revised Audiovisual Media Services Directive (AVMSD) was enacted in 2018; it imposed more obligations on video-sharing platforms as a specific PIS. Video-sharing platforms were tasked to take appropriate and proportionate measures, preferably through co-regulation, to protect the public from illegal content (terrorist content, child sexual abuse material, racism and xenophobia or other hate speech) and minors from harmful content.

The EU has developed a system for liability for content posted on the internet that differs from the US CDA230 immunity rules.[6] The central element is Section 4 of the ECD, entitled 'Liability of intermediary service providers'. Of the three sets of rules, the first two ('mere conduit' and 'caching') give PISs immunity from liability similar as under the US regime. More interesting, however, is the issue of the liability of hosting providers, for which rules have been included in Article 14 of the ECD. The (relative) novelty of the

---

3 Perry Keller, 'The New Television without Frontiers Directive' in Eric M. Barendt (ed), *Yearbook of Media and Entertainment Law. Volume III: 1997/98* (Clarendon Press, 1998, Oxford) 188, DOI: https://doi.org/10.1093/oso/9780198265979.003.0007

4 Perry Keller, *European and International Media Law: Liberal Democracy, Trade and the New Media* (Oxford University Press 2011, Oxford) 125, DOI: https://doi.org/10.1093/acprof:oso/9780198268550.003.0015

5 Gergely Gosztonyi, 'Aspects of the History of Internet Regulation from Web 1.0 to Web 2.0' (2022) 12 (1) Journal on European History of Law 168–173.

6 Anu Bradford, *Digital Empires. The Global Battle to Regulate Technology* (Oxford University Press 2003, Oxford) DOI: https://doi.org/10.1093/oso/9780197649268.001.0001

European system is the commonly used *notice and take-down system* (NTDS[7]), which has introduced a multi-step procedural system: the intermediary service provider must have specific knowledge of content that is manifestly illegal and must take steps to remove it expeditiously. In contrast to the US legislation, the EU has opted for a different model (also known as the *safe harbour model*[8]), which focuses on a non-automatic exemption.

In addition to the NTDS, the provisions of Article 15 of the ECD should be highlighted[9] that the Member States shall not impose a general obligation on service providers[10] to A) monitor the information which they transmit or store or B) actively seek facts or circumstances indicating illegal activity (no general obligation to monitor).[11] This rule, therefore, does not oblige service providers, and therefore nor social media, to monitor continuously the content posted on their sites.[12] It should be remembered, however, that the directive was created in 2000 and that, in the 2020s, more and more Member States have considered changing this rule. In 2015, however, the Manila Principles on Intermediary Liability, issued by NGOs, reaffirms in its principle I(d) the maintenance of the general ban on monitoring. As Senftleben and Angelopoulos stated, 'The saga of the general monitoring prohibition has indeed proven Odyssean'.[13]

III General Monitoring in the Practice of the CJEU

It is worth observing how the CJEU has tackled this issue in the meantime and helped to fill the gaps in the legislation with robust legal development work. The 'most important cases' list starts with the French cosmetics company L'Oréal, which reported to the online marketplace eBay that counterfeit versions of its products have been sold under the L'Oréal

---

7 Alexandre de Streel and others, *Online Platforms' Moderation of Illegal Content Online* (European Parliament 2020, Brussels) 10.

8 Tambiama Madiega, *Reform of the EU liability regime for online intermediaries: background on the forthcoming Digital Services Act* (European Parliamentary Research Service 2020, Brussels) 1–2.

9 Jan Oster, *European and International Media Law* (Cambridge University Press 2017, Cambridge) 234–236.

10 Aleksandra Kuczerawy, *Intermediary Liability and Freedom of Expression in the EU: from Concepts to Safeguards* (Intersentia 2018, Brussels) 63.

11 It is important to note, though, that the Article 'shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information' ECD Article 14(3).

12 Joris van Hoboken and others, *Hosting intermediary services and illegal content online. An analysis of the scope of article 14 ECD in light of developments in the online service landscape: final report* (European Commission 2018, Luxembourg) 45–47.

13 Martin Senftleben, 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* (University of Amsterdam – University of Cambridge 2020, Amsterdam – Cambridge) 7.

brand name on several occasions. The marketplace prohibits the sale of counterfeit goods in contracts signed by its users. As a result, the cosmetics company has held eBay (and in particular, its European operating subsidiary eBay.co.uk) liable. At the same time, it has also sued Google, which, after searching for the name of the cosmetic products, also displayed ads for those counterfeit products on eBay that were promoted for sale. In the case, Judge Arnold, sitting in the United Kingdom, raised several options that eBay could choose to filter out or minimise problems without generally monitoring the uploaded content.[14] The English court eventually referred the matter to the CJEU, the decision of which led many (such as Christine Riefa[15]) to conclude that operators should have a general obligation to monitor. However, in 2011 the CJEU did not take such a view in the formal documents in the case.[16]

A couple of years later, in 2016, in *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH*, Tobias Mc Fadden ran a shop in Germany selling light and sound equipment and also offered his customers free access to a wifi network, which was not password protected. In its judgment, the CJEU stated that, although it is for the national court to administer justice under federal and EU law, of the three technical solutions hypothetically proposed by the national court (withdrawal of the service, password protection or a general obligation to monitor traffic[17]), only password protection could pass the test of legality.[18]

In the 2019 case of *Eva Glawischnig-Piesczek v Facebook Ireland Limited,* the CJEU had to rule directly on Article 15 of ECD, unlike in previous instances where the general prohibition of monitoring was only raised as a sub-issue. Whereas previously, in the above points and the two SABAM cases,[19] the CJEU had also concluded that general monitoring was not an expectation for service providers, here there was a slight change of direction.[20] A defamatory text about the Austrian MEP Eva Glawischnig-Piesczek was published with a photo of her on Facebook. The person concerned not only asked the service to remove the content in question but also to remove all similar content (with the same content). The national court ordered the service provider to do the same. However, this can only

---

[14] *L'Oréal SA v eBay International AG* [2009] RPC 21, [2009] ETMR 53, [2009] EWHC 1094 (Ch), para 277.

[15] Christine Riefa, 'The end of Internet Service Provider's liability as we know it – Uncovering the consumer interest in CJEU Case C-324/09 (L'Oréal/eBay)' (2012) 1 (2) Journal of European Consumer and Market Law 104–111 DOI: https://doi.org/10.1007/s13590-012-0006-x

[16] Case C-324/09 *L'Oréal SA and others v eBay International AG and others,* ECLI:EU:C:2011:474.

[17] Case C-484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH,* ECLI:EU:C:2016:689, para 87.

[18] Gergely Gosztonyi, 'The contribution of the Court of Justice of the European Union to a better understanding the liability and monitoring issues regarding intermediary service providers' (2020) 59 (1) Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae – Sectio Iuridica 142, DOI: https://doi.org/10.56749/annales.elteajk.2020.lix.7.133

[19] Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),* ECLI:EU:C:2011:771; Case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV,* ECLI:EU:C:2012:85.

[20] Miriam Buiten, 'The Digital Services Act: From Intermediary Liability to Platform Regulation' (2021) 12 (5) Journal of Intellectual Property, Information Technology and E-Commerce Law 370, DOI: https://doi.org/10.2139/ssrn.3876328

be done if the service provider continuously monitors the content uploaded to it, so the national court referred the matter to the CJEU.[21] It held that the Member States have the possibility not only to require that the content in question be removed but also to impose such requirements on any similar content that may be shared *(notice-and-stay down).*[22] In this case, the court held that automated methods[23] could adequately address the issues raised: this is not general monitoring but only specific monitoring, according to the CJEU.[24] However, it should be stressed that the CJEU did not find[25] a clear dividing line between prohibited general monitoring and ad hoc monitoring measures.[26]

Overall, it seems that, in the time between the L'Oréal case in 2011 and the *Eva Glawischnig-Piesczek* case in 2019, the CJEU has made a minor change of direction, and although it referred to case-by-case monitoring, it seems to have shifted towards adopting general monitoring when analysing the case.[27] As Gyetván summarised, 'the arguments put forward in the judgments as a whole paint a rather worrying picture as regards the interpretation and enforcement of the prohibition of general monitoring'.[28]

IV General Monitoring in the EU Legislation after the ECD

In general, EU institutions increasingly perceived PISs as active internet guardians, the role of which is to detect and remove illegal content posted online.[29] The opinion that

---

[21] João Pedro Quintais, Sebastian Felix Schwemer, 'The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?' (2022) 13 (2) European Journal of Risk Regulation 199, DOI: https://doi.org/10.1017/err.2022.1

[22] Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited,* ECLI:EU:C:2019:821, para 36.

[23] Herbert Zech, 'General and specific monitoring obligations in the Digital Services Act' (2021) VerfBlog, <https://verfassungsblog.de/power-dsa-dma-07> accessed 15 December 2023, DOI: https://doi.org/10.17176/20210902-113002-0

[24] *Eva Glawischnig-Piesczek,* para 34.

[25] Alexandre de Streel, Miriam Buiten, Martin Peitz, *Liability of online hosting platforms: should exceptionalism end?* (Centre on Regulation in Europe 2018, Brussels) 20.

[26] Golunova also points out about the worrying aspect of CJEU's 'uncharacteristic ignorance of fundamental rights concerns'. Valentina Golunova, 'In Tech we Trust? Fixing the Evolutionary Interpretation by the Court of Justice of the Prohibition of General Monitoring in the Era of Automated Content Moderation' in Evangelia Psychogiopoulou, Susana de la Sierra (eds), *Digital Media Governance and Supranational Courts: Selected Issues and Insights from the European Judiciary* (Edward Elgar Publishing 2022, Cheltenham) 62.

[27] It should be noted though that Recital 30 of the DSA upholds this distinction between general monitoring obligations and monitoring obligations in specific cases.

[28] Dorina Gyetván, 'Az általános nyomon követési kötelezettség mint a közvetítő szolgáltatók felelősségének jövője? [A general monitoring obligation as the future of intermediary service providers' liability?]' in Marianna Fazekas (ed), *Jogi Tanulmányok 2021* (Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Kar, Állam- és Jogtudományi Doktori Iskola 2021, Budapest) 311.

[29] E.g. Proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, COM (2018) 640 final.

PISs should fulfil their role more actively is expressed in many EU acts and documents encouraging them to adopt effective proactive measures[30] that include automated means (e.g. filtering technologies).[31] EU institutions refer directly to automatic detection and filtering as measures that PISs may apply,[32] and underline the importance and encourage the development thereof.[33] At the same time, the EU legislators are obviously aware that the borderline between activities encouraging the application of automatic detection and filtering technologies as an instrument to tackle illegal content more actively and the prohibition of monitoring is very vague.[34] This is probably why the reference to Article 15 of the ECD is made very often to emphasise that instruments promoted by the EU within the field of tackling illegal content online cannot lead to general monitoring obligations.[35] On the other hand, it is difficult to identify instruments that PISs could apply to fulfil their obligations imposed upon them in the EU law without engaging in constant monitoring of online content, even if one bears in mind that the EC strongly underlines the voluntary nature of the proactive measures they implement.[36]

Two acts – the Copyright Directive (CDSMD)[37] and Regulation on Terrorist Content (TERREG)[38] – constitute examples of a struggle to reflect new expectations of the PISs in tackling illegal content online on the one hand and the prohibition of Article 15 of the ECD on the other. The legislative procedures thereof lead to the conclusion that the EC presents a relatively liberal attitude towards the prohibition of general monitoring obligations and a very flexible interpretation of its boundaries. On the other hand, the EP and the Council

---

30 Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online Towards an enhanced responsibility of online platforms, COM (2017) 555 final, 3.3.1.

31 Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online [2018] OJ L63/50.

32 Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry [2006] OJ L378/72.

33 COM (2017)/ 555 final.

34 Martin Husovec, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules' (2024) 38 (3) Berkeley Technology Law Journal 883–920, DOI: https://doi.org/10.2139/ssrn.4598426

35 E.g. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2017] OJ L 88/6.

36 Commission Recommendation (EU) 2018/334, 24.

37 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 L130/92; Joao Pedro Quintais, Christian Katzenbach, Sebastian Felix Schwemer et al., 'Copyright Content Moderation in the European Union: State of the Art, Ways Forward and Policy Recommendations' (2024) 55 (1) International Review of Intellectual Property and Competition Law 157–177, DOI: https://doi.org/10.1007/s40319-023-01409-5

38 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 L172/79.

make efforts to place the EC's proposals within the structure of the online liability regime constituted in the provisions of the ECD.

The EC's proposal of CDSMD[39] in its Article 13 required information society service providers whose services consist of the storage and provision to the public of access to large amounts of works or other subject matter uploaded by their users to put in place measures to ensure the functioning of agreements concluded with rightsholders for the use of their works or other subject-matter, or to prevent the availability on their services of works or other subject-matter identified by rightsholders. Among these measures, the EC listed effective content recognition technologies, which triggered wide criticism in the legal literature. Many authors argued that there would be general monitoring obligations imposed upon PISs. Christina Angelopoluos emphasised that the obligation to apply technologies of this kind would require precise general monitoring: after all, how can infringing content be *effectively recognised* on a platform using a technological tool without the oversight of the totality of the content on that platform?[40] To *recognise* unwanted content within a collection of content, one must logically examine each piece of content in that collection. Also, Frosio rightly observed that, by promoting automatic infringement assessment systems, the EC, in fact, would force PISs to develop and deploy filtering systems, therefore de facto monitor their networks and thus contradicting Article 15 of the ECD.[41] Stalla-Bourdillon and others argued that requiring PISs to use automated means, such as Content ID-type technologies, to detect systemically unlawful content, in fact, forces them to monitor all the data of each of their users actively and thereby amounts to a general monitoring obligation.[42]

Since the EC's proposal raised serious concern over its conformity with online liability regime,[43] the notion of content recognition technologies was removed during the legislative procedure.[44] The adopted Article 17 of the CDSMD provides new obligations for information society service providers, among which two are particularly interesting from the perspective of general monitoring. Firstly, PISs should obtain authorisation from the rightsholders, for instance, by concluding a licensing agreement, to communicate or make available to the

---

[39] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM (2016) 593 final.

[40] Christina Angelopoulos, *On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market* (University of Cambridge 2017, Cambridge) DOI: https://doi.org/10.2139/ssrn.2947800

[41] Giancarlo Frosio, 'To To Filter or Not to Filter? That is the Question in EU Copyright Reform' (2018) 36 (2) Cardozo Arts & Entertainment Law Journal 101–138.

[42] Sophie Stalla-Bourdillonand and others, 'Open Letter to the European Commission – On the Importance of Preserving the Consistency and Integrity of the EU Acquis Relating to Content Monitoring within the Information Society' (2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2850483> accessed 15 December 2023.

[43] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market – Orientation debate on Articles 11 and 13, 2016/0280 (COD).

[44] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market – Consolidated Presidency compromise proposal, 2016/0280 (COD).

public works or other subject matter (Article 17(1)). Secondly, if no authorisation is granted, information society service providers have to ensure the unavailability of specific works and other subject matter for which the rightsholders have provided relevant and necessary information (Article 17(4)(b)) and, in any event, shall act expeditiously, upon receiving a sufficiently substantiated notice from the rightsholders, to disable access to or to remove from their websites the notified works or other subject matter and make best efforts to prevent their future uploads in accordance with point (b) (Article 17(4)(c)).

Removing infamous *content recognition technologies* did not erase doubts regarding Article 17 of the CDSMD's compliance with a general monitoring obligation prohibition.[45] The problem is that its provisions, in fact, force information society service providers to verify all the content on the platform to determine if authorisation is required.[46] Gerald Spindler argues in this respect that, as a result, PISs must check the legality of the content itself and explicitly cannot rely on specific details provided by others.[47] This, without doubt, leads to the infringement of prohibition from Article 15 ECD. Also, provisions in Article 17(4)(b) and (c) of the CDSMD seem doubtful in the light of general monitoring, especially the first one that requires PISs to apply measures to avoid the availability on their services of unauthorised works and other subject matter. There are voices in the literature stating that Article 17(4)(b) of the CDSMD respects that there is no proactive obligation of providers to monitor their platforms, because the wording of Recital 66 CDSMD indicates that a PIS must fulfil its obligations from Article 17(4)(b) only on the basis on information provided by the rightsholder. In other words, the rightsholder's specific activity triggers a specific monitoring obligation of the PIS. It is worth noting, however, that the legislator does not indicate in the CDSMD what measures PISs should apply to fulfil their obligations. The provisions in question merely indicate that PISs should act under high industry standards of professional diligence. Moreover, the EC emphasises that information society service providers may implement here any relevant solutions, and it clearly refers to a free choice of available technology that allows the detection of unauthorised content, such as content recognition technology.[48] As a result, there is an increase in applications by some information

[45] Folkert Wilman, 'Two emerging principles of EU internet law: A comparative analysis of the prohibitions of general data retention and general monitoring obligations' (2022) 46 (1) Computer Law & Security Review DOI: https://doi.org/10.1016/j.clsr.2022.105728

[46] Eduardo Celeste and others, 'Shaping Standards from Below: Insights from Civil Society' in Eduardo Celeste and others (eds), *The Content Governance Dilemma. Information Technology and Global Governance* (Palgrave Macmillan 2023, Cham) 74, DOI: https://doi.org/10.1007/978-3-031-32924-1_4

[47] Gerald Spindler, 'The Liability system of Art. 17 DSMD and national implementation Contravening prohibition of general monitoring duties?' (2019) 10 (3) Journal of Intellectual Property, Information Technology and E-Commerce Law 344–374.

[48] Commission, Communication from the Commission to the European Parliament and the Council. Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market, COM (2021) 288 final.

society service providers of automated filtering tools.[49] Also, from the perspective of legal doctrine, this is a logical consequence of Article 17 of the DSDM. Montagnani and Trapova raised concerns that it is highly likely that whenever licensing agreements from Article 17 are not feasible, to avoid direct liability for violation of the right of communication to the public, information society service providers will resort to monitoring mechanisms.[50]

In its TERREG proposal, the EC presented the opinion that measures adopted based on provisions thereof may exceptionally derogate from the prohibition of imposing a general monitoring obligation. By stating this directly, the EC slightly opened the gate to instruments that can amount to general monitoring. Following this path, the EC imposed upon every PIS an obligation to detect terrorist content online actively, using proactive measures including automated means. During the legislation procedure, the EP noticed that the TERREG proposal would lead to infringement of the ECD.[51] The notion of proactive measures was therefore replaced by specific measures that include appropriate technical and operational measures or capabilities, such as proper staffing or technical means to identify and expeditiously remove or disable access to terrorist content (Article 5(2)(a)). Technical means of identifying terrorist content are interesting because they can also include filtering technologies. It leads to the conclusion that the EP simply replaced proactive measures constantly promoted by the EC with a different vocabulary.

Contrary to the EC's proposal, the provisions of TERREG are based on the dependence between the requirement to apply special measures to identify terroristic content and preceding decisions taken by competent state authorities. The EU legislator considers decisions from Article 5 TERREG to be special measures permitted in light of Article 14(3) of the ECD. It is doubtful, however, that the mere fact that obligations from Article 5 are connected with a decision of state authority would be sufficient here, even if it is addressed to certain PISs and concerns only a specific period of time. Despite such restrictions, this still may lead to general monitoring obligations. If they were to fulfil the requirements of Articles 14(3) and 15 of ECD, decisions from Article 5 of TERREG should be applicable in a specific case (to specific content) and be limited in time. This means they should indicate the duration of monitoring and information relating to the nature of the infringements in question, their author and their subject. Those elements are all linked with each other.[52] Decisions from Article 5 of TERREG do not fulfil these requirements due to their too general nature, which forces PISs to analyse various postings by their users to identify

---

[49] Jasmin Brieske, Alexander Peukert, *Coming into Force, not Coming into Effect? The Impact of the German Implementation of Art. 17 CDSM Directive on Selected Online Platforms* (University of Glasgow 2022, Glasgow) DOI: https://doi.org/10.2139/ssrn.4016185

[50] Maria Lillà Montagnani, Alina Trapova, 'New Obligations for Internet Intermediaries in the Digital Single Market – Safe Harbors in Turmoil?' (2019) 22 (7) Journal of Internet Law 3–19 DOI: https://doi.org/10.2139/ssrn.3361073

[51] COM (2018) 640 final.

[52] *Eva Glawischnig-Piesczek,* paras 44–47; 49–50.

terrorist content. Moreover, such analysis also requires an assessment of a content's nature, wording and context (TERREG Article 1(3)); this, in turn, contradicts the CJEU's opinion.

In the next section, we will point to how the above-discussed attempts, on the one hand, avoid general monitoring obligations and, on the other, follow a more practical need to find a pragmatic and functional system of redress and protection of rights, as has been reflected or mirrored in the final version of DSA.

V Debates on General Monitoring on the Path to the DSA-DMA

Because the European Union adopted the new and long-awaited digital services legislation in the summer and autumn of 2022, we discuss this final shape as an example of the final design of general monitoring obligations within the DSA. Digital Services regulation includes both DSA and Digital Markets Act (DMA).[53] We focus here on the DSA as a regulation primarily concerned with the liability of PISs for illegal content, online disinformation or other societal risks, transparency and consumer protection. In contrast, DMA primarily targets the lack of competition in digital markets.[54] The DMA covers gatekeeper online platforms (platforms with a dominant online position that makes it hard for consumers to avoid). However, some gatekeeper online platforms are also covered in the DSA (but from a different perspective). Therefore, the DMA is still occasionally cited.

It may be helpful to recapitulate the critical issues of the debate that led to the final version of the DSA, especially, but not exclusively, regarding general monitoring obligations by PISs. This debate concerned the following issues, to which we also provided selected responses and highlighted the still unresolved issue of inconsistency in monitoring obligations. To recapitulate, the critical points in the professional debate on content monitoring obligations for online social content concerned the following topics:

a) There was discussion of the immediate impact on free expression rights – it tilted the balance of the intermediary liability rules toward greater restriction of speech.[55] Therefore, for example, the European Media Association suggested[56] that the correct approach would be to limit the prohibition to targeting minors or based on sensitive data on very large online platforms (VLOP). This is partially the case for the DSA, when all PISs have rather specific obligations in protecting minors (DSA Article 28, 34(d), 35(j), 44(j)). At the same

[53] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1.

[54] Zsolt Ződi, *Platformjog [Platform law]* (Ludovika Egyetemi Kiadó 2023, Budapest).

[55] Jack M. Balkin, 'Free Speech is a Triangle' (2018) 118 (7) Columbia Law Review 2011–2055, 2029.

[56] European Media Association, 'Joint final recommendations by European Media Associations for the concluding stage of the Digital Services Act trialogue negotiations in relation to online advertising rules' (2021) <https://www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2022/210422%20Media%20Coalition%20DSA%20final%20recommendations.pdf> accessed 15 December 2023.

time, the VLOPs and the Very Large Online Search Engines (VLOSE) have specific duties (DSA Section 5), some of which are directly or indirectly related to monitoring obligations.

b) There was a worry about the move towards privatised enforcement through algorithmic artificial intelligence (AI) without transparency and the appropriate safeguards for speakers and the general public.[57] However, opponents argued that the different types of notice and action mechanisms used to regulate online content differ in their impacts. If the requirements are adequately defined and followed, they can act as essential safeguards. Their actual effect, however, may vary tremendously, depending on the form they take and accompanying restrictions – preferably administered by courts.[58] This is indeed the case – the CJEU has been assigned a specific role regarding relevant decisions by the EC.

c) There was a concern by the broadly discussed issue of the over-removal of lawful content *(false positives)* or an under-removal of illicit content *(false negatives).*[59] However, according to some authors, this is already a reality within the unregulated power of the platforms.[60] De Gregorio suggested two solutions to this issue: A) the insertion of new procedural rights in the online environment, including the obligation to explain the reasons behind platforms' decisions, and B) the second solution will question the doctrine of horizontal effect to establish a mechanism to enforce constitutional rights *vis-à-vis* online platforms that operate in a global framework.[61] The DSA requests that 'the providers concerned should, for example, take reasonable measures to ensure that, where automated tools are used to conduct such activities, the relevant technology is sufficiently reliable to limit, to the maximum extent possible, the rate of errors' (DSA Recital 26).

d) There was an occasional objection that such a regulation may hinder innovation and competition by increasing the costs of operating an online platform.[62] This is true for smaller platforms, but simultaneously, the VLOPs and the VLOSEs create forms of oligopolies that hinder competition.

---

[57] Michal Lavi, 'Do Platforms Kill?' (2020) 43 (2) *Harvard Journal of Law and Public Policy,* 477; Giancarlo Frosio, 'From Horizontal to Vertical: An Intermediary Liability Earthquake in Europe' (2017) 12 (7) Journal of Intellectual Property & Practice 565–575 DOI: https://doi.org/10.1093/jiplp/jpx061

[58] Aleksandra Kuczerawy, 'From 'Notice and Take Down' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression' in Giancarlo Frosio (ed), *The Oxford Handbook of Intermediary Liability Online* (Oxford University Press 2019, Oxford) DOI: https://doi.org/10.1093/oxfordhb/9780198837138.013.27

[59] Daphne Keller, *Empirical Evidence of "Over-Removal" by Internet Companies under intermediary liability laws* (Stanford Law School 2020, Stanford).

[60] Katrina Geddes, 'Meet Your New Overlords: How Digital Platforms Develop and Sustain Technofeudalism' (2020) 43 (4) Columbia Journal of Law and the Arts 455–485.

[61] Giovanni De Gregorio, 'From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society' (2018) 11 (2) European Journal of Legal Studies 65–103.

[62] Stefan Grundmann, Philipp Hacker, 'Digital Technology as a Challenge to European Contract Law – From the Existing to the Future Architecture' (2017) 13 (3) European Review of Contract Law 255–293, DOI: https://doi.org/10.1515/ercl-2017-0012; Elvira Caterina Parisi, Francesco Parisi, 'Rethinking Remedies for the Attention Economy' (2023) 31 (1) The Economics and Regulation of Digital Markets, DOI: https://doi.org/10.1108/S0193-589520240000031004

A general overview of a global debate on the regulation of the PISs was given by Školkay.[63] He showed that there were available ideas on regulating PISs, specifically the VLOPs. These measures included soft regulation, hard law and financial, technological and other direct and indirect regulatory mechanisms. In the end, within the EU, the solution was found in a rather detailed and extensive hard law regulation – the Digital Services Package. However, arguably, some other aspects included in that Package lead this regulation to having a hybrid status (e.g. some forms of co-regulation are included).

VI General Monitoring Obligations in the DSA – A Cornerstone of EU Digital Services Regulation

Article 8 of the DSA (No general monitoring or active fact-finding obligations) – based on a 2021 study, which drafted six policy options for an efficient EU liability system[64] – states that PISs are exempted from general monitoring obligations; however, there are two specific cases apart from this available exemption when monitoring can be required – either by national authorities[65] or in particular cases. For the former situation, on the one hand, there are checks provided by the EU legislation (including the DSA) – as specified by the CJEU. 'The applicable Union legislation' is first mentioned only in general terms and only later the more specific relevant and related EU legislation (TERREG, Regulation (EU) 2019/1020[66] and Regulation (EU) 2017/2394[67]) are mentioned.

On the other hand, national authorities are defined quite broadly – they may include 'national judicial or administrative authorities, including law enforcement authorities' (DSA Recital 31). Again, a balance seemed to be sought in the sense that there is actually no general monitoring possible by national authorities. Still, instead, case-by-case intervention is possible. National authorities 'may order providers of intermediary services to act against one or more specific items of illegal content or to provide certain specific information' (DSA Recital 31). Specific cases include content considered illegal in the offline world (which is

63 Andrej Školkay, 'An Exploratory Study of Global and Local Discourses on Social Media Regulation' (2020) 10 (1) Global Media Journal (German Edition) 1–51, DOI: https://doi.org/10.22032/dbt.44942

64 Andrea Bertolini, Francesca Episcopo, Nicoleta-Angela Cherciu, *Liability of online platforms* (European Parliamentary Research Service 2021, Brussels).

65 An example could be the KEHTA system (Központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisa, Central database of electronic inaccessibility decisions) operated by the Hungarian National Media and Infommunications Authority. See: <https://adatkapu.nmhh.hu>.

66 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 [2019] OJ L169/1.

67 Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004, [2017] OJ L345/1.

also the general philosophy of this regulation). This questions the legal philosophy that initially, as discussed earlier, tried to treat online regulation as fundamentally different from the offline world (yet, in hindsight, slowly moving away from non-regulation to soft regulation and co-regulation as well as hard regulation).[68]

The territorial scope of monitoring is probably the most challenging issue. There is a clear general rule (DSA Recital 36) that 'the effect of the order should, in principle, be limited to the territory of the issuing Member States'. There are again two exceptions to this general rule: A) 'unless the illegality of the content derives directly from Union law' (for example, this can be related to copyright or terrorist content); and B) if 'the issuing authority considers that the rights at stake require a broader territorial scope'. The latter definition is clearly too broad, as it allows any intervention abroad, as the regulation 'does not provide the legal basis for issuing such orders, nor does it regulate their territorial scope or cross-border enforcement' (DSA Recital 31). This questions the actual effectiveness of the DSA in such cases, which is ultimately limited to national law, which is determined by international agreements.

Nevertheless, again, there is a strong right given to the national authorities: 'The obligation for the orders to contain a statement of reasons explaining why the information is illegal content may be adapted where necessary under the applicable national criminal procedural laws' (DSA Recital 34). Even more strongly, 'Therefore, where those laws in the context of criminal or civil proceedings provide for conditions that are additional to or incompatible with the conditions provided, (…) they might not apply or might be adapted' (DSA Recital 34). This may allow another free space for legal interpretation. Indeed, national authorities (or, in effect, Member States) should not be affected by the possibility 'to require a provider of intermediary services to prevent an infringement' concerning illegal content (DSA Recital 34).

An exciting and vital aspect tackles language issues when issuing and communicating orders. The DSA (Recital 35) suggests that: 'the transmission of the order should be accompanied by a translation of at least the elements of the order which are set out in this Regulation' if there is no previous agreement on the use of language and if the language used by the provider of intermediary services is different from the EU official languages. This may concern Chinese or Russian PISs as well.[69]

VII Conclusion

The prohibition of general monitoring has been kept in the final DSA regulation. However, monitoring obligations have been impacted by a need to produce regulations that satisfy

[68] Petra Lea Láncos, *The Many Facets of EU Soft Law* (Pázmány Press 2022, Budapest). DOI: https://doi.org/10.4337/9781802208917

[69] Gergely Gosztonyi, 'Special models of internet and content regulation in China and Russia' (2021) 9 (2) ELTE Law Journal 87–99, DOI: https://doi.org/10.54148/ELTELJ.2021.2.87

all key players. This, by necessity, a typical EU approach, included many internal checks and balances, including some vague wordings, within the DSA concerning monitoring options. Moreover, not surprisingly, monitoring as specified in the DSA seems to be heavily influenced by previous legal discussions, case law and experiences with soft law.

As a result, one must be very careful when thinking about the DSA. As mentioned, there is a general exemption from monitoring obligations. This is highlighted by the wording 'neither *de iure* nor *de facto*'. This is quite strong wording, providing further guarantees against national security and intelligence agencies' illegal or special monitoring. The text of the DSA allows a lot of interventions and creative interpretation by national authorities – especially if relevant national legislation to which the DSA is referring is somewhat vague or when national authorities are less liberally-minded.[70]

Moreover, the EU's regulatory approach[71] may lead to doubts that it applies *contra lege* interpretation of the prohibition of monitoring, which also opposes the case law of CJEU. The EU regulatory solution created a situation in which, in the light of binding provisions in Article 15 of the ECD, PISs are obliged to tackle illegal content actively. The EC imposed these obligations in legal acts and using legally non-binding documents (self-regulatory or co-regulatory guidelines).

Although the EU regulation underlines the importance of the prohibition of imposing general monitoring obligations upon PISs, at the same time, it fundamentally undermines this very principle. The EC's regulatory initiatives are in effect, leading to a situation that is inconsistent with the established liability regime. Although the DSA pretends that obligations that amount, for instance, to applying filtering technologies do not infringe the prohibition from Article 15 of ECD, even the nature of such measures brings doubts about their consistency with the current liability regime. One may get the impression that the DSA expects that PISs will apply filtering technologies to detect illegal content online in general, acting voluntarily but at the same time construing legal obligations in a way that leaves them with no choice and merely forces them to monitor all content coming from various users, thereby infringing the law.

However, one should admit that PISs, at least the VLOPs and the VLOSEs, already use filtering technologies to detect illegal content online, but the question is whether this should be treated as a justification for an ever-spreading inconsistency in the EU's regulatory approach. For many years, the position of PISs was built on a well-established liability regime based on their reaction to illegal content online.

Despite the new DSA provisions, we should not forget that 'even if providers were to make an effort to properly evaluate all proactively discovered content before taking action on it, they would still face incredible difficulties due to inconsistent speech laws around the

[70] Ondřej Moravec and others, 'Digital Services Act Proposal (Social Media Regulation)' (2021) 14 (2–3) Studia Politica Slovaca 166–185, DOI: https://doi.org/10.31577/SPS.2021-3.5

[71] Anupam Chander, 'When the Digital Services Act Goes Global' (2023) 38 (4) Berkeley Technology Law Journal, DOI: https://doi.org/10.15779/Z38RX93F48

globe'.[72] In a few years, the EU legislation has moved to proactive detection and removing such illegal and also charmful content. Based on co-regulatory measures, the current DSA considers tackling 'the possible negative impacts of systemic risks on society and democracy,[73] such as disinformation or manipulative and abusive activities' (DSA Recital 104).[74]

So now the question is which regime is to follow in the coming years for online PIS liability?

[72] Golunova (n 26) 56.

[73] János Tamás Papp, *A közösségi média szabályozása a demokratikus nyilvánosság védelmében [Social media regulation to protect the democratic public]* (Wolters Kluwer 2022, Budapest).

[74] It should be noted that DMA that is not discussed in detail here, even strengthened traceability and checks on traders to ensure products and services are safe. This includes steps to perform random checks on whether illegal content resurfaces among its marketed goods.