Gesellschaft für Freiheitsrechte

Article 17 of the Directive on Copyright in the Digital Single Market: a Fundamental Rights Assessment

Julia Reda, Joschka Selinger & Michael Servatius

16 November 2020

This study is licensed as:
Creative Commons CC-by 4.0 international
Gesellschaft für Freiheitsrechte e.V.

About GFF: Gesellschaft für Freiheitsrechte e.V. (Society for Civil Rights) is a Berlin-based non-profit NGO founded in 2015. Its mission is to establish a sustainable structure for successful strategic litigation in the area of human and civil rights in Germany and Europe. The GFF's current cases focus on protecting privacy, freedom of information and the press, and defending equal freedom for all.

Table of Contents

Executive Summary

Article 17 of the Directive on Copyright in the Digital Single Market (CDSMD) makes certain online platforms directly liable for copyright infringements of their users. The provision as a whole is internally contradictory, leaving Member States with the difficult task of reconciling its different, fundamentally incompatible requirements.

In order to avoid liability, platforms will have no other choice but to employ content recognition technologies (upload filters) in order to demonstrate that they have made best efforts to automatically block uses of protected works on the request of rightsholders. The use of those technologies constitutes a prohibited general monitoring obligation.

The Republic of Poland has brought an action for annulment of certain provisions of Article 17 CDSMD before the CJEU (Case C-401/19), arguing that those provisions violate the fundamental right to freedom of expression and information.

The case before the Court has far-reaching implications beyond the realm of copyright law, as similar sector-specific legislation is being considered in other areas, and the European Commission is in the process of drafting horizontal legislation on content moderation.

The case *Poland v European Parliament and Council* only addresses a small part of the provisions of Article 17 CDSMD that could be in violation of the Charter. Even a failure of the action would be insufficient to conclude that Article 17 CDSMD is compatible with primary law. While Poland has only raised concerns regarding the violation of the fundamental right to freedom of expression and information, the Court is entitled to a comprehensive assessment of the provisions in question, balancing all fundamental rights concerned.

Article 17 CDSMD fails to strike a fair balance between the right to intellectual property of rightsholders and the freedom of expression and information of users, their right to privacy and the freedom to conduct a business of platform operators.

The use of upload filters will invariably lead to ex-ante restrictions on legal forms of expression, a particularly egregious interference with the right to freedom of expression and information. The CJEU and the ECtHR have consistently rejected measures that lead to the automated blocking of legal expression. Article 17 CDSMD lacks specific provisions to define the scope of fundamental rights restrictions and fails to provide for the necessary minimum safeguards. To the extent that safeguards against the blocking of legal expression are included in Article 17 CDSMD, those safeguards lack enforcement provisions

Article 17 CDSMD violates the freedom to conduct a business of the affected platform operators. The legislator failed to consider the shortcomings of content recognition technologies, underestimated their cost and left the scope of the best efforts obligations placed on platforms entirely unclear. The proportionality principle included in Article 17 (5) CDSMD is an insufficient safeguard for the freedom to conduct a business.

Article 17 CDSMD fails to adequately protect the users' right to privacy, in particular by subjecting them to fully automated decisions regarding their communications on the affected platforms.

1 Introduction

Article 17 of Directive 2019/790 on Copyright in the Digital Single Market (CDSMD) constitutes a paradigm shift not just for copyright law, but also for intermediary liability in Europe more generally. So far, the responsibility of hosting service providers for illegal acts of their users has generally been a question of secondary liability[1], which has not been harmonized by the European legislator beyond the liability limitations enshrined in section 4 of Directive 2000/31/EC on electronic commerce (ECD).

Article 17 CDSMD makes a subset of hosting service providers directly liable for copyright infringements of their users and is widely considered to require the use of upload filters, which would place ex-ante restrictions on the ability of users to communicate via these platforms. Its adoption was accompanied by widespread protests by citizens[2], as well as criticism from academics[3] and fundamental rights advocates[4]. While Member States are in the process of implementing Article 17 CDSMD into their national laws, the European institutions are deliberating additional sector-specific legislation that raises similar questions about the fundamental rights implications of filtering technologies.[5] The controversy around Article 17 CDSMD has led the European Parliament to view these technologies much more critically than in the past, and express strong reservations against their use.[6]

---

[1] A few judgements by the CJEU have assigned primary liability to hosting service providers in strictly delineated circumstances. For an explanation of how this case law differs from the liability regime introduced by Article 17 CDSMD, see *Reda,* Article 17: What is it really good for? Rewriting the history of the DSM Directive. Kluwer Copyright Blog. https://perma.cc/7KDQ-A3ZQ.

[2] Approximately 170,000 people participated in street protests against the adoption of the DSM Directive on 23.03.2020. Cf. *Reuter,* Demos gegen Uploadfilter: Alle Zahlen, alle Städte. https://netzpolitik.org/2019/demos-gegen-uploadfilter-alle-zahlen-alle-staedte/.
Over five million signed a petition against Article 17 CDSMD called "Stop the censorship-machinery! Save the Internet!" on the public participation platform change.org. https://www.change.org/p/european-parliament-stop-the-censorship-machinery-save-the-internet.

[3] Numerous open letters from academics and European research institutes to the legislators at different stages of the legislative process, criticizing Article 17 CDSMD (then Article 13), are available at: EU Copyright Reform, Evidence on the Copyright in the Digital Single Market Directive. UK Copyright and Creative Economy Centre, University of Glasgow. https://www.create.ac.uk/policy-responses/eu-copyright-reform/.

[4] Cf. United Nations. Office of the High Commissioner on Human Rights. Letter of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye to the European Commission of 13.06.2020. OL OTH 41/2018. https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-OTH-41-2018.pdf.

[5] Cf. Proposal for a Regulation of the European Parliament and the Council on preventing the dissemination of terrorist content online. COM(2018) 640 final. Article 6.

[6] *"The European Parliament […] 5. Stresses that the responsibility for enforcing the law must rest with public authorities; considers that the final decision on the legality of user-generated content must be made by an independent judiciary and not a private commercial entity; […] 12. Takes the firm position that the Digital Services Act must not oblige content hosting platforms to employ any form of fully automated ex-ante controls of content unless otherwise specified in existing Union law, and considers that mechanisms voluntarily employed by platforms must not lead to ex-ante control measures based on automated tools or upload-filtering of content and must be subject to audits by the European entity to ensure that there is compliance with the Digital Services Act"*, European Parliament. Report with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online. (2020/2019(INL))

Against this background, the action brought before the Court of Justice of the European Union by the Republic of Poland,[7] requesting the annulment of parts of Article 17 CDSMD on the grounds that they violate users' fundamental right to freedom of expression and information, is of particular importance. This study aims to make a contribution to the academic assessment of Article 17 CDSMD and in particular its compliance with the Charter of Fundamental Rights. The authors hope that this study will not just inform the debate on Article 17 CDSMD, but also shed light on the fundamental rights implications of the increased reliance on automated law enforcement mechanisms operated by private actors more generally.

The structure of Article 17 CDSMD and its numerous internal contradictions, which have given rise to significant academic debate over its interpretation, are the subject of chapter 2. Chapter 3 goes on to examine the scope of the action for annulment of specific provisions of Article 17 CDSMD before the CJEU and the standard of review applied by the Court to actions brought by Member States for the annulment of provisions of secondary EU law.

Chapters 4 to 6 loosely follow the structure of the specific questions raised by the Court in the public hearing on *Poland v European Parliament and Council* that took place on 10 November 2020. The hearing dealt with four questions: 1) to what extent Article 17 CDSMD requires the use of upload filters, 2) the risks posed by the use of such technologies for the freedom of expression and information of users, 3) the scope of the obligation on platforms to block user-uploaded content, namely whether that obligation is limited to manifestly infringing uses of protected material and 4) the compatibility of Article 17 CDSMD with the requirements set by the CJEU regarding the responsibility of the European legislator to define fundamental rights safeguards in Union legislation.[8] In chapter 4, we show that Article 17 CDSMD introduces a prohibited general monitoring obligation. The impact of that obligation on the fundamental right to freedom of expression and information is analysed in chapter 5. Chapter 6 addresses the EU legislator's obligation to establish fundamental rights safeguards in EU law.

Chapter 7 and 8 deal with fundamental rights not explicitly raised by the plaintiff in *Poland v European Parliament and Council*, but which are nevertheless of particular importance for the Court's assessment of the compatibility of the specific provisions of Article 17 CDSMD with the Charter. The impacts of Article 17 CDSMD on the freedom to conduct a business of service providers (chapter 7) and the right to data protection of users (chapter 8) are examined in detail, given the importance of those fundamental rights in underpinning the ban on general monitoring obligations.[9] Chapter 9 draws conclusions on the legality of Article 17 CDSMD and automated filtering obligations more generally.

[7] CJEU, C-401/19, Action brought on 24 May 2019 – *Poland v European Parliament and Council*.
[8] CJEU, C-311/18, ECLI:EU:C:2020:559 – *Facebook Ireland v Schrems*, para 175.
[9] CJEU, Judgement of 24-11-2011, C-70/10, ECLI:EU:C:2011:771 – *Scarlet*; CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog*.

2 Structure and Contradictions of Article 17

The normative content of Article 17 CDSMD leads to irresolvable contradictions.[10] Article 17 CDSMD contains 10 paragraphs, some of which consist of relatively vague general principles, whereas others contain detailed specifications. The substantive contents of the individual paragraphs are partly in tension with each other. The provisions do not contain clear instructions as to how these tensions are to be resolved. Moreover, the norm is concretized by numerous, unusually extensive recitals.[11] In parts, these serve more to obfuscate than to elucidate the meaning of the legislative provisions.

The specifications of Article 17 CDSMD must be considered in the context of the legislator's regulatory concern: At the turn of the millennium, the European legislator adopted the E-Commerce Directive (ECD), which limited service providers' liability for illegal acts of their users.[12] This regime "has underpinned the development of the Internet in Europe"[13] by creating a legal framework that enabled innovation in the field of online services. It also encouraged the creation of digital environments in which users could exercise their fundamental right to freedom of expression. Increasingly, copyright industry groups as well as some academics have started questioning whether these provisions are still appropriate given the changing role of at least some service providers such as YouTube.[14] This concern has entered the EU copyright reform debate under the keyword 'value gap'.

Despite its origins as a measure intended to address this concern, Article 17 CDSMD has undergone significant changes between the initial legislative proposal presented by the European Commission in 2016[15] and its eventual adoption in 2019. Many of these changes were introduced in response to significant public criticism of its potential impact on fundamental rights. Those changes form an integral part of the final political agreement, even if some Member States try to present them as secondary to the true purpose of the provision.[16] Article 17 CDSMD as adopted nevertheless changes the liability requirements for a certain subset of hosting service providers, called online content-sharing service providers (OCSSPs). Consequently, Article 17 (3) CDSMD sets out that the safe harbour provisions of Article 14 (1) ECD do not apply within the boundaries of Article 17 CDSMD.

---

[10] See *Samuelson,* Pushing Back on Stricter Copyright ISP Liability Rules, Michigan Technology Law Review, Forthcoming, p. 3 summarizes that Article 17 CDSMD is internally contradictory, deeply ambiguous, and harmful to small and medium-sized companies as well as to user freedoms of expression. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3630700.

[11] Then again, the recitals are silent on important matters, e.g. how to understand Article 17 (5) CDSMD, see ibid., p. 13.

[12] See *Angelopouos,* On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market, p. 9 for a comparison of the hosting safe harbour in the E-Commerce Directive and the notice-and-takedown system under the US Digital Millennium Copyright Act.

[13] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*,* A digital single market strategy for Europe, {SWD(2015) 100 final}, No. 3.3.2.

[14] *Quintais*, The New Copyright in the Digital Single Market Directive: A Critical Look, European Intellectual Property Review 2020(1), p 17.

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

[16] Cf. Communia Associaton, Article 17 guidance: Don't shoot the messenger / ne pas tirer sur le messager! https://perma.cc/6AQE-WTUS.

The starting point for the new liability regime is Article 17 (1) CDSMD. According to this provision, an OCSSP performs an act of communication to the public or an act of making available to the public when it gives the public access to large amounts of copyright-protected works or other protected subject matter uploaded by its users. The definition of an OCSSP, which paves the way for the liability, is to be found in Article 2 (6) CDSMD.[17] As this definition encompasses services that have not been considered to be performing acts of communication to the public within the meaning of Art 3 (1) InfoSoc Directive with regards to information uploaded by their users,[18] it must be concluded that Article 17 (1) CDSMD constitutes a sui generis extension of the right to communication to the public.[19] Consequently, every OCSSP in principle must obtain an authorisation for those acts of communication to the public – for example by concluding a licensing agreement with the rightsholder.

This basic principle of primary liability is mitigated by a new much stricter liability mitigation mechanism, found in Article 17 (4) and (5) CDSMD. In the absence of an authorisation, OCSSPs are exempted from liability if three conditions are met in combination: Firstly, they must have made best efforts to obtain an authorisation (lit. a)).[20] Secondly, it is necessary that they have made best efforts to ensure the unavailability of specific protected content for which rightsholders have provided the relevant and necessary information (lit. b)). Which efforts are required is determined by high industry standards of professional diligence. Lastly, once a rightsholder provides an OCSSP with a sufficiently substantiated notice, the provider must act expeditiously to disable access to that content and make best efforts to prevent future uploads in accordance with lit. (b). These two obligations result from lit. c). If the provider does not fulfill these requirements, it is liable for the violation of the rightsholders' exploitation rights.

Article 17 (5) CDSMD makes the aforementioned obligations subject to the principle of proportionality and specifies particular criteria to be taken into account during the proportionality assessment. Article 17 (6) CDSMD introduces lighter obligations for startups, which will be of limited significance due to the narrow definition of OCSSPs that can benefit from this regime.

Despite the reference to proportionality, the requirements of Article 17 (4) CDSMD are generally considered to constitute an obligation to use filtering technologies to meet the requirements of the paragraph. [21] Even if the Directive does not explicitly mention filtering technologies, Article 17 CDSMD at least gives platform operators a strong incentive to implement such tools in order to limit their liability.[22] It may even be argued that the

[17] The vagueness of the definition leads to ambiguities, *Samuelson,* Pushing Back on Stricter Copyright ISP Liability Rules, Michigan Technology Law Review, Forthcoming, p. 17. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3630700.

[18] Cf. *Reda*, Article 17: What is it really good for? Rewriting the history of the DSM Directive. Kluwer Copyright Blog. https://perma.cc/7KDQ-A3ZQ.

[19] Cf. *Husovec/Quintais,* How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3463011.

[20] Cf. for criticism on this provision: *Spindler*, Art. 17 DSM-RL und dessen Vereinbarkeit mit primärem Europarecht, GRUR 2020, pp 258 ff.

[21] *Schwemer/Shovsbo*, What is Left of User Rights? Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime, Forthcoming in Paul Torremans (ed), Intellectual Property Law and Human Rights, 4th edition, 2020, p. 5. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3507542.

[22] *Husovec*, Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p 14.

requirement is implicitly derived from the substantive requirements of the provision.[23] As will be shown, Member States' implementation proposals thus far clearly support the prediction that upload filters will become mandatory. We will discuss this central requirement of the Article 17-regime and its significant implications for users' and platform operators' fundamental rights in more detail below. At this point, it shall already be stated that Article 17 CDSMD leads to nothing less than a paradigm shift: Whereas up until now protected content was available unless shown to be infringing, now materials that are detected by algorithms will be removed from public circulation unless demonstrated to be legitimate.[24]

The paragraphs that set out the new liability regime for OCSSPs are followed by provisions aimed at limiting the impact of the OCSSPs' obligations on the rights of the users.[25] Article 17 (7) CDSMD provides that the cooperation between OCSSPs and rightsholders shall not cause content lawfully uploaded by users to be unavailable. In other words, legal content shall not be blocked. This should in particular apply when the use is covered by an exception or limitation. Users must be able to rely on exceptions or limitations for quotations, criticism and review, as well as for caricature, parody or pastiche. Recital 70 clarifies that these exceptions and limitations are thereby rendered mandatory. *Samuelson* argues that Article 17 (7) CDSMD is one of several serious internal contradictions of the overall provision, as it cannot be brought in accordance with the obligations set out in Article 17 (4) CDSMD.[26] At least, it is not clear how far the OCSSPs obligation to safeguard these requirements goes.[27] If taken literally, any restriction of availability would be prejudicial in relation to Article 17 (7) CDSMD. Such an understanding is supported by the systematic argument that Article 17 (7) CDSMD is formulated as an abstract, objectively defined obligation. In contrast, Article 17 (4) CDSMD is based on the "best efforts" of the operators and thus seems to introduce a more subjective obligation.[28] From this a comparatively user-friendly interpretation can be derived, according to which providers must let a disputed upload be available in cases of doubt.[29]

However, given the fact that Article 17 CDSMD does not clarify the relative importance of its conflicting provisions, Member States are discussing different approaches to national implementation. It is becoming apparent that many of them consider the provisions of Article

---

[23] Cf. *Grisse,* After the storm – examining the final version of Article 17 of the new Directive (EU) 2019/790, Journal of Intellectual Property Law & Practice, 2019, Vol. 14, No. 11, p 894 with further references.

[24] *Elkin-Koren*, Fair Use by Design, UCLA Law Review 64 (2017), p 1093; *Schwemer/Shovsbo*, What is Left of User Rights? Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime, Forthcoming in Paul Torremans (ed), Intellectual Property Law and Human Rights, 4th edition, 2020, p. 15. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3507542.

[25] *Grisse,* After the storm – examining the final version of Article 17 of the new Directive (EU) 2019/790, Journal of Intellectual Property Law & Practice, 2019, Vol. 14, No. 11, p 897.

[26] *Samuelson* Pushing Back on Stricter Copyright ISP Liability Rules, Michigan Technology Law Review, Forthcoming, p. 14. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3630700.

[27] See the recommendation of *Quintais et al.* Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics, 10 (2020) JIPITEC 277.

[28] This distinction is not as clear in all language versions of the Directive. Most versions contain a wording which translates as "all efforts". See *Rosati,* DSM Directive Series #5: Does the DSM Directive mean the same thing in all language versions? The case of 'best efforts' in Article 17 (4)(a). https://ipkitten.blogspot.com/2019/05/dsm-directive-series-5-does-dsm.html.

[29] This viewpoint was in particular defended by the Commission and the Council in the hearing regarding the case C-401/19 (*Poland v Parliament and Council*). See the report of *Keller* CJEU hearing in the Polish challenge to Article 17: Not even the supporters of the provision agree on how it should work. Kluwer Copyright Blog. https://perma.cc/8D8K-V7MZ.

17 (7) CDSMD to be of secondary importance at best. This issue is exacerbated by the fact that in many language versions of the directive, the term "best effort" is translated in a manner that suggests an objective rather than a subjective obligation.[30] Furthermore, it is practically impossible to fulfil the goal of Article 17 (7) CDSMD in total. This assumption is supported by the existence of Article 17 (9) CDSMD, which describes what should happen when legal content does get blocked. Consequently, some Member States seem to understand Article 17 (7) CDSMD as little more than an aspirational statement, which does not require any independent implementation, but would be realised in the complaint and redress mechanism of Article 17 (9) CDSMD.[31]

Article 17 (9) CDSMD contains procedural safeguards in order to institutionalize a system of checks and balances.[32] It requires Member States to provide that OCSSP "put in place an effective and expeditious complaint mechanism". Complaints under this mechanism "shall be processed without undue delay, and decisions to disable access to or remove uploaded content shall be subject to human review". Rightsholders requests to make content unavailable have to be "duly justified". It is unclear whether these requirements on human review of blocking decisions and on the justification of blocking requests apply at the outset, or only after a user has made a complaint. The Member States are furthermore required to put in place out-of-court redress mechanisms for the impartial settlement of disputes "without prejudice to the rights of users to have recourse to efficient judicial remedies".

All of these requirements affect not the substantive dimension of copyright – i.e. the exceptions and limitations –, but the way the rights are exercised.[33] These measures affect several levels, namely the platform level, the out-of-court level, and the judicial authority or court level. Ultimately, these specifications confer upon users a subjective right to enforce exceptions and limitations.[34] Therefore, the existence of these safeguards somewhat implies that Article 17 (7) CDSMD notwithstanding, Article 17 (4) CDSMD will inevitably lead to

---

[30] See *Rosati,* DSM Directive Series #5: Does the DSM Directive mean the same thing in all language versions? The case of 'best efforts' in Article 17 (4)(a). https://ipkitten.blogspot.com/2019/05/dsm-directive-series-5-does-dsm.html. Most drastically, this is reflected in the discussion about the French implementation where Article 17 (7) CDSMD is not transposed at all. The German proposal (Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz zum Entwurf eines Gesetzes zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes) illustrates that the declared goal will not be achieved in a variety of constellations. To name just two examples: Users are practically, at least directly, not able to quote in large scale, with over 90% concordance, Section 12 (2) UrhDaG-E. Secondly, content will be in the first instance removed if the rightholders' request for blocking is only made after the upload by the users, §§ 8, 10 UrhDaG-E.

[31] Consultation related to the European Commission's future guidance on the application of article 17 on the Copyright in the digital single market directive, Non paper from Croatia, Denmark, France, Greece, Italy, Portugal and Spain. https://www.communia-association.org/wp-content/uploads/2020/10/201027non-paper.pdf.

[32] *Quintais*, The New Copyright in the Digital Single Market Directive: A Critical Look, European Intellectual Property Review 2020(1), p. 19.

[33] *Schwemer/Shovsbo*, What is Left of User Rights? Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime, Forthcoming in Paul Torremans (ed), Intellectual Property Law and Human Rights, 4th edition, 2020, p. 12. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3507542.

[34] *Specht-Riemenschneider*, Leitlinien zur nationalen Umsetzung des Art. 17 DSM-RL aus Verbrauchersicht, pp 88 f. See also *Schwemer/Shovsbo*, What is Left of User Rights? Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime, Forthcoming in Paul Torremans (ed), Intellectual Property Law and Human Rights, 4th edition, 2020, pp 9 ff., 12 f., who extrapolate this from recent CJEU case law. , https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3507542.

situations where platforms will falsely remove or block legitimate content.[35] This has led some commentators to conclude that in accordance with the mentioned paradigm shift in relation to Article 17 (4) CDSMD, the *ex-ante* review mechanism changes to an *ex-post* mechanism.[36] The opposite interpretation is also possible, however, given that Article 17 (9) subpara 3 CDSMD declares that the Directive shall in no way affect legitimate uses, such as uses under exceptions or limitations. This general postulate is in inherent contradiction to the practical understanding that the legislator expressed for the norm through the aforementioned specifications.

The matter is further complicated by Article 17 (8) CDSMD, which stipulates that the application of Article 17 CDSMD may not lead to any general monitoring obligation.[37] This provision contradicts the obligations of Article 17 (4) CDSMD, which appears to require platforms to engage in general monitoring in order to escape liability.[38] Since the Court has established that this prohibition is required by the Charter of Fundamental Rights (CFR), this study dedicates an entire chapter to the examination of the compatibility of Article 17 CDSMD with the ban on general monitoring obligations.

It is left to the Member States to try to reconcile these wildly contradictory elements of Article 17 CDSMD when trying to transpose the provision into national law.[39] The problem is exacerbated by the fact that the requirements are very vague in many areas. These circumstances do not just raise the question whether Article 17 CDSMD meets the requirements of the Charter, but also whether it constitutes a step towards the Directive's stated goal of harmonizing the Digital Single Market.[40]

3 Standard of Review in the CJEU Case

Poland seeks the annulment of Article 17 (4)(b) CDSMD and of parts of Article 17 (4)(c) CDSMD. The CJEU is examining the extent to which these provisions on the liability exemption regime are compatible with primary law, in particular the fundamental rights of the CFR. The applicant explicitly invokes the incompatibility with the freedom of expression and information guaranteed by Article 11 CFR, which it attributes to the fact that the regulations require service providers to carry out prior automatic verification, i.e. filtering. Poland argues this would undermine the essence of the aforementioned fundamental rights and would not comply with the requirement that limitations imposed on that right be proportional and necessary.

---

[35] *Schwemer/Shovsbo*, What is Left of User Rights? Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime, Forthcoming in Paul Torremans (ed), Intellectual Property Law and Human Rights, 4th edition, 2020, p 14. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3507542.

[36] *Frosio*, Reforming the C-DSM Reform: A User-Based Copyright Theory for Commonplace Creativity, p. 17. https://ssrn.com/abstract=3482523 ; *Schwemer/Shovsbo*, What is Left of User Rights? Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime, Forthcoming in Paul Torremans (ed), Intellectual Property Law and Human Rights, 4th edition, 2020, p. 16. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3507542.

[37] Article 17 (8) CDSMD.

[38] See the detailed analysis in chapter 4.

[39] *Husovec/Quintais,* How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms, p. 3. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3463011.

[40] See *Samuelson*, Pushing Back on Stricter Copyright ISP Liability Rules, Michigan Technology Law Review, Forthcoming, p. 22. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3630700.

It is to be welcomed that Poland has initiated the legal proceedings. This enables the CJEU to examine the standard for the compatibility of the aforementioned elements of Article 17 CDSMD with fundamental rights at an early stage. Nevertheless, the legal challenge is quite narrow in that it only concerns Article 17 (4)(b) and (c) *in fine*. Poland's approach results in the CJEU being barred from reviewing other provisions of Article 17 CDSMD. This is regrettable, as the scientific community has raised potential collisions of other substantive provisions with primary law.[41] For example, Article 17 (3) CDSMD excludes OCSSPs from the hosting safe harbour enshrined in Article 14 (1) ECD, although the EU has committed itself to maintaining those safe harbours through numerous international trade agreements.[42]

If the CJEU were to conduct a comprehensive examination of all elements of Article 17 CDSMD, it would inadmissibly broaden the scope of the plaintiff's petition and deprive the defendant of the opportunity to defend itself properly.[43] The fact that Poland alternatively requests the annulment of Art. 17 CDSMD in its entirety in case that the challenged provisions are inseparably connected with the provision only relates to the legal consequence but not to the examination program. As a consequence, even if Poland's action should fail, this would be insufficient to conclude the compatibility of Article 17 CDSMD as a whole with primary law.

Of course, the substantive content of the provisions under review can only be properly understood in relation to the liability regime of Article 17 CDSMD in total. Against this background it is necessary to investigate the provisions within their regulatory context. As the questions posed by the Court in the hearing of 10 November 2020 demonstrate, the interpretation of potential fundamental rights safeguards contained in other provisions of Article 17 CDSMD is central to the overall assessment.[44]

The significant public controversy over Article 17 CDSMD may have motivated Poland to file the action before the CJEU mere days before the 2019 European Parliament was elected.[45] In this case, the urgency could explain the rather narrow scope of the action, not just with respect to the specific provisions of Article 17 CDSMD, but also with respect to the relevant fundamental rights. [46] This possibility should not, however, affect the assessment of the action's merits.

In any case, the CJEU is not required to limit its assessment to the compatibility of the challenged provisions with the freedoms guaranteed in Art. 11 CFR. In the action for

[41] See e.g. *Spindler,* GRUR 2020, 253, 257 ff. with regard to Art. 17 (1) and (4)(a) CDSMD.
[42] See for example the Free Trade Agreement between the EU and the Republic of Korea (OJ 2011, L 127/6). In the section on enforcement of IP rights (Sec. C), the FTA contains rules on the liability of online service providers that largely correspond to those of the E-Commerce Directive (Sub-Sec. B). This concerns in particular the liability of hosting service providers, Art. 10.65 FTA.
[43] See *Dörr* in Grabitz/Hilf/Nettesheim 71st ed., 2018, Art. 263 TFEU paras 150, 197.
[44] Cf. *Keller,* CJEU hearing in the Polish challenge to Article 17: Not even the supporters of the provision agree on how it should work. Kluwer Copyright Blog. https://perma.cc/8D8K-V7MZ.
[45] *Schwemer/Shovsbo*, What is Left of User Rights? Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime, Forthcoming in Paul Torremans (ed), Intellectual Property Law and Human Rights, 4th edition, 2020, fn. 4. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3507542.
[46] *Schwemer/Shovsbo*, consider it to be an interesting fact that Poland did not invoke the freedom to conduct business, Ibid. fn. 6.

annulment, the CJEU objectively and comprehensively examines the challenged provisions.[47] The plaintiff has not only the right but also the duty to specify which provisions are the subject of the proceedings.[48] However, the plaintiff is not entitled to limit the examination of the provision to its compatibility with particular fundamental rights through certain specifications. Such a limitation would be unreasonable, as it would preclude a balancing of all relevant fundamental rights by the Court in the case of a collision of different competing rights.[49] The fact that the application may not be based on a comprehensive legal examination or that the plaintiff limited itself to criticizing only certain interferences does not prevent the CJEU from a complete examination. It is even necessary to comprehensively review the provisions in dispute with regard to their overall compatibility with primary law.

It follows from the case law of the CJEU that a balance must be established between the fundamental rights affected.[50] Member States, when transposing a directive, must rely on an interpretation which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order.[51] In a copyright context, the protection of the fundamental right to property, which includes intellectual property, must be balanced against the protection of other fundamental rights.[52] Such a fair balance requires amongst other things that the principle of proportionality is met, which requires that measures implemented through Community provisions have to be appropriate for attaining the objective pursued and must not go beyond what is necessary to achieve it.[53] In unclear cases, the interpretation that gives the best consideration to the conflicting fundamental rights is to be favored.[54] Article 17 CDSMD clearly concerns the fundamental right to intellectual property, however this right is not absolute. The CJEU has stated that the use of (intellectual) property may be regulated in so far as is necessary for the general interest.[55] The case law has not yet specified in detail how this balance is to be achieved. The Court, in essence, finds its conclusion by considering the effects of the disputed mechanisms and weighing up the consequences for all parties involved.

[47] *Cremer* in Calliess/Ruffert, 5th ed., 2016, Art. 263 TFEU para 86; with such an approach also *Peters/Schmidt,* Das Ringen um Upload-Filter geht in die 2. Runde*,* GRUR Int. 2019, p 1004.
[48] See *Ehricke* in Streinz, 3rd ed., 2018, Art. 263 TFEU para 29.
[49] CJEU, C-70/10, ECLI:EU:C:2011:771 – *Scarlet*, para 44. See also CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog*, para 50 f.
[50] CJEU, C-275/06, ECLI:EU:C:2008:54 – *Promusicae*, para. 68. See *Stieper* in Schricker/Loewenheim, 6th ed., 2020, before §§ 44a ff. UrhG para 32; *Wandtke/Hauck* NJW 2017, 3422, 3424; *Leenen* in Wandtke/Bullinger, 5th ed., 2019, preface InfoSoc Directive, para 32.
[51] CJEU, C-275/06, ECLI:EU:C:2008:54 – *Promusicae*, para. 68.
[52] CJEU, C-70/10, ECLI:EU:C:2011:771 – *Scarlet*, para. 44; CJEU, C-275/06, ECLI:EU:C:2008:54 – *Promusicae*, paras. 62 ff.
[53] CJEU, C-479/04, ECLI:EU:C:2006:549, *Laserdisken ApS*, para. 53. See *Leenen* in Wandtke/Bullinger, 5th ed., 2019, preface InfoSoc Directive, para 34.
[54] *Stieper* in Schricker/Loewenheim, 6th ed., 2020, before §§ 44a ff. UrhG para 32 with Reference to CJEU, Judgement of 26-04-2012, C-510/10, ECLI:EU:C:2012:244 – *DR and TV2 Danmark A/S*, para 57.
[55] CJEU, C-277/10, ECLI:EU:C:2012:65 – *Luksan*, para. 68. See also *Leenen* in Wandtke/Bullinger, 5th ed., 2019, preface InfoSoc Directive, para. 32.

4 Article 17 Constitutes a General Monitoring Obligation

In its plea, the Republic of Poland claims that Article 17 (4) (b) and (c) CDSMD require OCSSPs to perform preventive automated verification of user-uploaded content in order to avoid liability by blocking material which infringes copyright. This necessity, according to the applicant, violates the essence of the right of freedom of expression and information guaranteed by Article 11 CFR. The CJEU has ruled on the compatibility of filtering obligations in a number of cases revolving around the ban on general monitoring obligations as set out in Article 15 (1) ECD. In its case-law, the CJEU has grounded the ban on general monitoring in fundamental rights law – not merely in Article 11 CFR, which is the subject of the Polish plea, but also in the freedom to conduct a business of the service provider (Article 16 CFR), and the service users' right to protection of personal data (Article 8 CFR) – because a filtering system would fail to strike a fair balance between the right to intellectual property on the one hand and the competing fundamental rights of service providers and users on the other hand.[56] In order to assess the compatibility of Article 17 CDSMD with the Charter, it is therefore relevant whether Article 17 (4)(b) and (c) CDSMD constitute a prohibited general monitoring obligation.

In order to answer this question, it is necessary to analyse which obligations on service providers are prohibited by the ban on general monitoring obligations and, consequently, the Charter of Fundamental Rights, in the context of copyright enforcement. In a second step, one must ascertain whether Article 17 CDSMD requires OCSSPs to introduce such prohibited general monitoring practices.

4.1 Scope of the Ban on General Monitoring

The ban on general monitoring as set out in Article 15 (1) ECD has been the subject of extensive interpretation by the Court. The E-Commerce Directive is a legislative instrument that applies horizontally regardless of the nature of illegal content in question. Therefore, when determining whether Article 17 CDSMD violates the ban on general monitoring, and consequently the Charter, a uniform interpretation of the scope of the ban on general monitoring is required that is compatible with all relevant judgements.

Three major competing interpretations of the ban on general monitoring are present in the literature, which shall be examined in detail. Only one of those interpretations meets the requirement of reconciling the different considerations that the Court has presented when interpreting the ban on general monitoring in its case-law. In this chapter, these competing interpretations shall be examined and applied to obligations on hosting service providers in the field of copyright law in order to draw conclusions for the application of the ban on general monitoring to the obligations under Article 17 CDSMD.

4.1.1 Option 1: Upload Filters Must Be Specific Regarding the Copyrighted Work

According to this interpretation, the ban on general monitoring only prohibits abstract obligations to detect previously unknown illegal activity, for example the use of techniques such as sentiment analysis, machine learning, or human observation of user-uploaded

[56] CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog*, paras. 46 ff.

content. The identification of known copyright-protected works that the rightsholder has notified to the service provider, on the other hand, is qualified by proponents of this interpretation as "monitoring in a specific case", which is allowed according to recital 47 ECD[57].

The CJEU has consistently rejected such a narrow interpretation of the ban on general monitoring in its copyright-related case-law. In *Scarlet* (a case concerning an internet access provider) and *Netlog* (a case concerning a social network not unlike Facebook, except for its size), the Court ruled an obligation on an access provider and a hosting provider, respectively, to filter all or almost all user uploads for infringements of the repertoire of the Belgian collecting society SABAM to be incompatible with the ban on general monitoring. Arguments that this decision rested on the fact that the injunctions in question in those cases would have encompassed both the existing known catalogue work works represented by SABAM, as well as any infringements of its unknown future repertoire,[58] are indefensible. First of all, both judgements concerned the filtering of works "*in respect of which the applicant [SABAM] claims to hold [intellectual property] rights*".[59] The reference, in both cases, to a claim by SABAM, indicates that the injunction in question was never intended to extend to current or future works in SABAM's repertoire to which it had not claimed rights. Furthermore, it is clear from the judgement in the main proceedings of the Scarlet case that the dispute concerned an injunction requiring Scarlet to install the content filtering service Audible Magic,[60] which operates solely on the basis of reference files provided by rightsholders and which was explicitly mentioned by the European Commission in its impact assessment for the CDSMD as one of the filtering technologies that OCSSPs could be expected to employ.[61]

When determining that the injunctions in dispute in *Scarlet* and *Netlog* constituted general monitoring obligations, the Court did not consider whether the burden would be on the service provider to find out whether the works in question were indeed part of SABAM's repertoire. Instead, the Court characterized an injunction as a prohibited general monitoring obligation if it required the monitoring of all or almost all communications by all users, as a preventive measure, unlimited in time and at the sole expense of the service provider.[62]

Even if one were to follow the argument outlined above that the monitoring obligations in *Scarlet* and *Netlog* were insufficiently precise regarding the works that service providers would be required to identify, the Court's ruling in *McFadden* makes it clear that even an injunction requiring the blocking of all infringements of a single work constitutes an impermissible general monitoring obligation. The Court unequivocally rejected an injunction requiring an internet access provider to block all infringements of Sony Music's rights in a single, pre-identified phonogram:

> *"As regards, first, monitoring all of the information transmitted, such a measure must be excluded from the outset as contrary to Article 15(1) of Directive 2000/31, which*

[57] Cf. *Leistner*, European Copyright Licensing and Infringement Liability Under Art. 17 DSM-Directive. ZGE, pp 123–215.
[58] Cf. ibid., p 140.
[59] CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog*, para. 25; CJEU, C-70/10, ECLI:EU:C:2011:771 – *Scarlet*, para. 29.
[60] Le cour d'appel de Bruxelles, 9ème chambre, 28.1.2010, R.G.: 2007/AR/2424.
[61] Commission Staff Working Document, Impact Assessment on the modernisation of EU copyright rules, SWD(2016) 301 final, section 5.2.3.
[62] Ibid.

excludes the imposition of a general obligation on, inter alia, communication network access providers to monitor the information that they transmit."[63]

The filtering obligations introduced by Article 17 (4)(b) and (c) CDSMD would go far beyond the scope of filtering rejected by the Court in *McFadden*. While these obligations only extend to works for which the rightsholders have provided OCSSPs with the "relevant and necessary information", it is reasonable to expect that the holders of rights in large repertoires of protected works and other subject-matter who are not interested in conducting a license agreement with an OCSSP will provide that OCSSP with reference files in order to block their entire repertoire of content on the service. The filtering obligations enshrined in Article 17 CDSMD are therefore more comparable to the situation in *Scarlet* and *Netlog*, i.e. the blocking of an entire repertoire, than with that in McFadden, which concerned the blocking of a single isolated work.

In any case, the interpretation that obligations to filter copyright-protected content are permissible specific monitoring as long as the subject-matter for which the service provider is monitoring has been notified by the rightsholder must be rejected as obviously incompatible with the case-law.

4.1.2 Option 2: Upload Filters Must be Specific Regarding the Work and the Infringer

It is clear from *McFadden* that when determining whether a monitoring obligation is general or specific, the Court does not merely consider whether the work *for* which a service provider is monitoring is specified, but also whether the obligation requires the service provider to monitor "all of the information transmitted" for a possible match with the known protected work. This has led some commentators to conclude that in order for a monitoring obligation to be specific and therefore in compliance with the Charter, it must specify not just the content to be identified, but also a specific subset of all users of the platform which are deemed to be potential infringers.[64] As an additional safeguard, the number of total blocking requests should be limited so as not to constitute a de facto general monitoring obligation when applied to different subsets of users of the service, which would cumulatively encompass all the platform's users. According to this interpretation, monitoring obligations that require a service provider to check all user uploads for a potential infringement, even when the obligation is limited to monitoring for infringements in a specific work, would always constitute a prohibited general monitoring obligation, as was the case in *McFadden*.

This interpretation of the case-law appears compatible with all rulings in the context of intellectual property infringements – not just the aforementioned copyright-related rulings, but notably also with *l'Oréal v eBay*, a trademark infringement case. In this case, the Court found that "the measures required of the online service provider concerned cannot consist in an active monitoring of all the data of each of its customers in order to prevent any future infringement of intellectual property rights via that provider's website. Furthermore, a general monitoring obligation would be incompatible with Article 3 of Directive 2004/48, which states

[63] CJEU, C-484/14, ECLI:EU:C:2016:689 – *McFadden*, para. 87.
[64] Cf. *Senftleben/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. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717022.

that the measures referred to by the directive must be fair and proportionate and must not be excessively costly."[65]

According to the interpretation outlined in chapter 4.1.1 above, one would have expected the Court to deem a monitoring obligation to be permissible as long as it was limited to the particular trademark of l'Oréal that was the subject of the case. Instead, the Court proposed, as a non-exhaustive list of permissible injunctions the suspension of the infringer's account, as well as measures to aid the identification of users selling products on eBay.[66] Both of these measures can be read as indications that the identity of the affected user plays an important role in determining whether an obligation can be deemed specific. This distinction is made explicit in *Tommy Hilfiger*, a trademark infringement case in the offline realm. In this judgement, the Court summarized its finding in *l'Oréal v eBay* as follows:

> *"By contrast, the intermediary may be forced to take measures which contribute to avoiding new infringements* ***of the same nature by the same market-trader*** *from taking place (see, to that effect, judgment of 12 July 2011 in L'Oréal and Others, C-324/09, EU:C:2011:474, paragraphs 138 to 141)"*[67](accentuation by the authors).

By contrast, the Court deemed that the illegality of a particular offer on sale cannot be determined by the mere presence of a trademark on that product, as there exist circumstances in which the sale of the product is legitimate even without the express permission of the trademark holder (e.g. when trademark protection on a product is exhausted). Therefore, an obligation to identify and block all uses of a single specified trademark would fail to strike a fair balance between the different competing rights.[68] The same is true for copyright protection: While the use of the same copyright-protected work may be unlawful by one user, it may be lawful by another, for example when that user has obtained a license or is the beneficiary of an exception or limitation. This holds true even when the context of the use is identical except for the identity of the user (i.e. when the whole work or the same extract of the work is reproduced by both users).

While the above interpretation of the ban on general monitoring as excluding all monitoring obligations that fail to identify a subset of users to be monitored appears compatible with all relevant judgements in the field of intellectual property, it is hard to reconcile with the Court's case-law on defamation. In *Glawischnig-Piesczek*, the court found an injunction permissible that requires the blocking of material that has previously been deemed illegal by a court, "*irrespective of who requested the storage of that information*".[69] While it is possible, as the proponents of this interpretation argue, that the standards for the ban on general monitoring are sector-specific[70], the horizontal nature of the E-Commerce Directive rather suggests a uniform interpretation of Article 15 (1) ECD.

---

[65] CJEU, C-324/09, ECLI:EU:C:2011:474 – *l'Oréal v eBay*, para. 139.
[66] Ibid., praras 141–142.
[67] CJEU, C-494/15, ECLI:EU:C:2016:528 – *Tommy Hilfiger*, para. 34.
[68] CJEU, C-324/09, ECLI:EU:C:2011:474 – *l'Oréal v eBay*, praras. 140, 143.
[69] CJEU, C-18/18, ECLI:EU:C:2019:821 – *Glawischnig-Piesczek*, para. 37.
[70] Cf. *Senftleben/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, pp. 14 f. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717022.

Glawischnig-Piesczek therefore casts serious doubt on this second interpretation of the ban on general monitoring, but it also fails to support the first reading, according to which the blocking on the basis of mere rightsholder notifications is permissible. Instead, the Court requires that in order for a monitoring obligation to be permissible, a court determine a specific communicative act to be illegal and to give clear instructions to the service provider, in the form of an injunction, on how to identify identical or essentially unchanged illegal content, without having to undertake an independent assessment of that content.[71] Obviously, Article 17 (4)(b) and (c) CDSMD would also fail to meet the requirements established by the Court in *Glawischnig-Piesczek*, as they contain no mention of a court injunction as a prerequisite for blocking alleged copyright infringements. A third interpretation of the ban on general monitoring is required in order to reconcile the seemingly incompatible statements made by the Court in its case-law on intellectual property rights infringement, on the one hand, and defamation, on the other hand.

4.1.3 Option 3: Upload Filters Must Be Specific Regarding the Infringement

A convincing reconciliation of the case-law on general monitoring obligations is presented by Advocate General Saugmandsgaard Øe in his opinion on the *YouTube* and *Cyando* cases.[72] This interpretation considers all monitoring obligations to be general which fail to specify particular illegal acts that are subject to the monitoring obligation. Unlike the interpretations of the ban on general monitoring set out above that require monitoring obligations in a copyright context to be specific regarding the *copyright-protected work* or the *infringer*, this interpretation requires monitoring obligations to be specific regarding the *infringement*.

In *Glawischnig-Piesczek*, the Court deemed monitoring obligations to be permissible only to the extent that a court had determined the defamatory nature of a particular statement and issued an injunction requiring the hosting service provider to block future uploads of the same statement. This obligation could only extend to equivalent statements to the one giving rise to the injunction insofar as the issuing court itself, in its injunction, had specified which other statements should be considered equivalent, so as to allow the hosting service provider to perform the monitoring obligation in a fully automated manner, without the need to perform an independent assessment of the illegality of content, and without any danger that legal content may be blocked in the process.[73]

The room for courts to issue such injunctions covering equivalent defamatory statements is quite narrow, given that the exact content of the equivalent statement must be specified in the injunction. It would be impermissible for a court to issue an injunction that required the blocking of all uploads that merely contained the defamatory statement, while adding additional statements that could provide context. Otherwise, there would be a significant danger that legal statements such as journalistic articles quoting from the defamatory

[71] CJEU, C-18/18, ECLI:EU:C:2019:821 – *Glawischnig-Piesczek*, paras. 39, 45.
[72] Advocate General Saugmandsgaard Øe, Opinion, Joined Cases C-682/18 and C-683/18, ECLI:EU:C:2020:586 – *YouTube* and *Cyando*.
[73] CJEU, C-18/18, ECLI:EU:C:2019:821 – *Glawischnig-Piesczek*, paras. 45 ff.

statements at issue in *Glawischnig-Piesczek* in an effort to discuss the consequences of the court ruling[74] would be unlawfully blocked in the process.

Applying the standard of *Glawischnig-Piesczek* to the field of copyright infringement, the Advocate General rightfully points out that copyright infringement (not unlike defamation, as we just discussed) is highly context-sensitive:

> *"While the illegal nature of some information is immediately obvious, that is not the case with copyright as a rule. The assessment of the infringing character of a file requires a number of contextual elements and may call for thorough legal analysis. For example, in order to establish whether a video uploaded on a platform such as YouTube infringes copyright it is necessary, in principle, to determine whether, first, the video contains a work, second, the complaining third party holds rights to that work, and third, the use made of the work infringes his or her rights, the latter point requiring an evaluation whether, in the first place, the use was made with his or her authorisation, and, in the second place, an exception is applicable. The analysis is further complicated by the fact that any rights and licences for the work are likely to vary from one Member State to another, as are the exceptions, according to what law is applicable."*[75]

An injunction to require the prevention of future copyright infringements would therefore only be permissible if, rather than covering all uses of a copyright-protected work, it only extended to *uses of a work* that are identical or equivalent to a use of the same work that had previously been found by the court to be infringing. According to the Advocate General, identical uses would be uses of the exact same file, whereas equivalent uses include files that use the protected work in the same way (for example showing an entire film without any additional contextual information present), but which may have been uploaded in a different file format.[76]

Senftleben and Angelopoulos, who favour the interpretation of the ban on general monitoring set out in chapter 4.1.2 above, criticize that this reading of *Glawischnig-Piesczek* is incompatible with the Court's case-law in *Scarlet*, *Netlog* and *McFadden*, because it deems permissible, under certain circumstances, the monitoring of all user uploads for a match with a specific infringement. They further question how the imposition of a blocking obligation by injunction would better protect the fundamental rights of users from the over-blocking that is inherent to filtering systems than in the context of a legislative notice-and-staydown obligation.[77] However, it is possible to reconcile the interpretation of the ban on general monitoring put forward by Advocate General Saugmandsgaard-Øe with the entirety of the case-law. Should the Court indeed decide that the standard of the *Glawischnig-Piesczek* judgement, which concerns defamation, can be applied to copyright cases, this decision would

---

[74] Examples of such journalistic articles abound, see for example: The New York Times, 27.06.2019, When a Politician Is Called a 'Lousy Traitor,' Should Facebook Censor It? https://www.nytimes.com/2019/06/27/opinion/facebook-censorship-speech-law.html.

[75] Advocate General Saugmandsgaard Øe, Opinion, Joined Cases C-682/18 and C-683/18, ECLI:EU:C:2020:586 – *YouTube* and *Cyando*, para. 188.

[76] Ibid., para. 221.

[77] Cf. *Senftleben/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, pp. 15 f. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717022.

still be compatible with the Court's previous interpretations of the ban on general monitoring obligations.

Crucially, according to the Advocate General, any blocking injunction must be sufficiently specific to only target illegal uploads. In other words, it must not "*prevent users of a platform from uploading legal content and, in particular, legally using the work concerned*".[78] Drawing upon the previous analysis of the context-sensitivity of copyright infringement, the possible blocking injunctions discussed in *Scarlet*, *Netlog* and *McFadden* would clearly fail to meet this requirement.

As discussed previously, even an identical use of a copyright-protected work that a court has deemed illegal when performed by one user can be legal when performed by another user. This fact excludes blocking injunctions for copyright-infringing material against Internet access providers such as Scarlet or McFadden at the outset. As the Advocate General points out, users must not be deprived of their right to private copying as set out in Article 5 (2)(b) InfoSoc Directive, which may be performed within the context of any Internet access service or cyberlocker.[79] Consequently, the mere finding that an infringement of the rights in a particular phonogram has occurred over such a service is not indicative of the illegality of future transmissions of the exact same material over the same service, because another user may be a beneficiary of an exception such as that for private copying, or indeed hold a license to use the work legally. A court would be unable to specify criteria that would allow Internet access providers to block, without the need for independent assessment, infringing uses of the work without also blocking legal uses of the work.

In the context of a hosting service provider such as Netlog or Facebook, it is conceivable that a rightsholder can demonstrate to a court that no user of that hosting service provider holds a license to make a particular work available to the public via that service. This would open the door for the court to issue an injunction that would only concern the blocking of uploads of publicly accessible identical or equivalent copies of the entire protected work in question, without any accompanying contextual information that could indicate the legality of the use under a copyright exception such as those for quotation according to Article 5 (3)(d) InfoSoc Directive or for educational purposes according to Article 5 (3)(a) InfoSoc Directive. The infringing character of such identical or equivalent uses of whole works without accompanying contextual information could be deemed apparent and an injunction that is limited to the blocking of such uses could be deemed permissible. The injunction would have to be limited to uploads accessible to the general public so as to rule out the possible application of the private copying exception.

The interpretation of the ban on general monitoring obligations as presented by Advocate General Saugmandsgaard Øe, is therefore compatible with the entirety of the Court's case-law on general monitoring. Due to the context-sensitivity of copyright law, where the difference between a legitimate use and an infringement can depend on both the context in which a work is used and on the person who is using the work, there is only very limited room for blocking injunctions against hosting service providers regarding publicly accessible copyright infringements.

---

[78] Advocate General Saugmandsgaard Øe, Opinion, Joined Cases C-682/18 and C-683/18, ECLI:EU:C:2020:586 – *YouTube* and *Cyando*, para. 222.
[79] Ibid., para. 222, fn. 11.

It is clear at the outset that Article 17 (4)(b) CDSMD is fundamentally incompatible with the ban on general monitoring following this interpretation. Firstly, it requires OCSSPs to make best efforts to block, not on the basis of a court injunction, but on the basis of information provided by a rightsholder. Neither the rightsholder nor the OCSSP, both acting for commercial purposes, is incentivized to undertake a balancing of the blocking request with the fundamental rights of users, as a court is required to do before issuing an injunction. Secondly, Article 17 (4)(b) CDSMD requires best efforts to block "specific works or other subject matter", rather than specific infringements. Indeed, unlike Article 17 (4)(c) CDSMD, this provision requires no connection whatsoever to a previous infringement on the OCSSP's services, so it's inconceivable that the "relevant and necessary information" provided by rightsholders as a basis for the OCSSP's blocking efforts would specify the particular infringing use to be blocked. Otherwise, there would be no distinction between Article 17 (4)(b) CDSMD, which refers to preventive blocking, and Article 17 (4)(c) CDSMD, which refers to notice-and-staydown.

Article 17 (4)(c) CDSMD is also difficult to reconcile with the ban on general monitoring. In order to be compatible, "a sufficiently substantiated notice from the rightsholders" would have to be interpreted as including a finding by a court that a particular use of the rightsholder's work or other protected subject-matter on the service of the OCSSP is indeed infringing. Even in that case, Article 17 (4)(c) CDSMD requires the blocking of access to "the notified *works or other subject matter*" (accentuation by the author), rather than the blocking of access to the notified (as well as identical or equivalent) *infringements*.

4.2 The Ban on General Monitoring in Article 17

Having confirmed that an obligation to automatically detect and block the use of copyright-protected works on the basis of relevant and necessary rightsholder information constitutes a prohibited general monitoring obligation within the meaning of Article 15 (1) ECD, it is necessary to determine whether Article 17 (4)(b) and (c) CDSMD indeed require such an obligation. The analysis in the previous subchapter indicates that this is the case, but it must first be determined that no alternative means of complying with the obligations under Article 17 (4)(b) and (c) CDSMD exist that would avoid general monitoring.

A textual interpretation of Article 17 (8) CDSMD would indicate that an interpretation of Article 17 (4)(b) or (c) CDSMD that results in a general monitoring obligation is ruled out.[80] However, the wording in Article 17 (8) CDSMD is narrower than that in Article 15 (1) ECD. It does not include the ban on "a general obligation actively to seek facts or circumstances indicating illegal activity". It is therefore unclear whether the legislator intended to merely reiterate that Article 15 (1) ECD applies to OCSSPs[81], even when they cannot benefit from the liability limitation of Article 14 (1) ECD for the purposes of Article 17 CDSMD, or whether the intention was to set a different standard. Given that the Court has confirmed that the protection of fundamental rights in accordance with the Charter requires a ban on general

[80] „The application of this Article shall not lead to any general monitoring obligation." Article 17 (8) first sentence CDSMD.

[81] It is worth pointing out that even if Article 15 (1) ECD did not apply to OCSSPs, primary EU law would still prohibit general monitoring obligations. Cf. Advocate General Saugmandsgaard Øe, Opinion, Joined Cases C-682/18 and C-683/18, ECLI:EU:C:2020:586 – *YouTube* and *Cyando,* para. 122, fn. 112.

monitoring, Article 17 CDSMD could fail to meet this standard if the ban on general monitoring as laid down in Article 17 (8) CDSMD provides a lower level of fundamental rights protection than that in Article 15 (1) ECD.

More importantly, commentators have cautioned that in practice, the obligations laid down in Article 17 (4) CDSMD leave providers with no other option than to introduce filtering systems that – based on the favourable interpretation described above – constitute general monitoring .[82] A legislative provision that asserts the ban on general monitoring, while placing obligations on OCSSPs that will invariably lead them to "voluntarily" engage in general monitoring in an effort to meet those obligations, also fails to meet the requirements of the Charter.

While the European Commission has stated in its draft guidance that "Member States should not mandate the use of technology or impose any specific technological solutions on service providers in order to demonstrate best efforts"[83], it is clear from several draft implementation proposals at national level that have been published thus far that several Member States intend to do just that. While some national governments intend to transpose the ban on general monitoring in Article 17 (8) first sentence CDSMD verbatim[84], the French[85] and German[86] implementation proposals contain no mention of it. Germany also omits the criterion of "best efforts" in its transposition of Article 17 (4)(b) and (c) CDSMD[87]. Both governments have indicated that they expect OCSSPs to use filtering technologies to fulfil their obligations under the draft laws. The French Ministry of Culture has commissioned a study on content recognition technologies, stating: "Article 17 of the new European directive on copyright in the digital market gives [content recognition technologies] an enhanced scope, by transforming these tools, put in place on a *voluntary* basis, into devices *called for by European Union law* and governed by it" (accentuation by the author).[88] The German Ministry of Justice has published a flowchart illustrating the functioning of its implementation proposal which requires the use of a reference database filled with reference files provided by rightsholders, as is characteristic of content recognition technologies using fingerprints or hashes to identify alleged copyright infringements.[89]

---

[82] *Angelopoulos/Quintais*, Fixing Copyright Reform: A Better Solution to Online Infringement. JIPITEC, Volume 10, Number 2.

[83] European Commission, Targeted consultation addressed to the participants to the stakeholder dialogue on Article 17 of the Directive on Copyright in the Digital Single Market, p. 8.

[84] For an overview of draft implementation proposals, see: Communia Association, DSM Directive Implementation Tracker. https://www.notion.so/DSM-Directive-Implementation-Tracker-361cfae48e814440b353b32692bba879.

[85] Ministère de la culture, Projet de loi relatif à la communication audiovisuelle et à la souveraineté culturelle à l'ère numérique.

[86] Bundesministerium der Justiz und für Verbraucherschutz, Referentenentwurf für das Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes.

[87] Ibid., Article 3, §§ 1, 10 and 11.

[88] "L'article 17 de la nouvelle directive européenne sur le droit d'auteur dans le marché numérique leur donne une portée renforcée, en transformant ces outils, mis en place de manière volontaire, en dispositifs appelés par le droit de l'Union européenne et encadrés par lui." Ministère de la culture, Lettre de mission rectificative du CSPLA sur les outils the réconnaissance des contenus protégés par les plateformes de partage en ligne. https://www.culture.gouv.fr/content/download/210530/file/Lettre%20de%20mission%20rectificative.pdf.

[89] Bundesministerium der Justiz und für Verbraucherschutz, 16. Oktober 2020, Grafik Öffentliche Wiedergabe und Vergütungen. https://perma.cc/AG6K-LMQJ.

The European Commission also concedes that "in most cases, it is expected that service providers will rely (or continue to rely)[90] on technological tools in order to comply with their obligation under Article 17 (4)(b)".[91] It becomes clear from the rest of the draft guidance that the Commission does expect OCSSPs to rely on those tools for fully automated blocking decisions at least in some cases, despite statements that Article 17 CDSMD does not impose a particular technological solution. The system proposed in the draft guidance aims at reducing, not eliminating, the erroneous blocking of legal uses of copyright-protected works by automated content filtering mechanisms, without providing similarly detailed instructions for any alternative means of compliance with Article 17 CDSMD that would not entail general monitoring. Insofar as the draft guidance document lists alternatives to upload filters based on fingerprinting technology,[92] these alternatives consist entirely of other technical means by which to perform general monitoring of user uploads, but they fail to list *alternatives to general monitoring*. In an interview, the responsible Director for Media Policy at the European Commission's Directorate General for Communications Networks, Content and Technology has gone so far as calling content recognition technologies such as fingerprinting "fundamental" for the practical application of Article 17 CDSMD.[93]

It is clear from these statements by the European Commission and from the implementation proposals at national level available today that Article 17 CDSMD will impose general monitoring by OCSSPs. This raises the question whether the European legislator can evade its fundamental rights obligations by making general monitoring only de facto mandatory, without specifying alternative options available to OCSSPs to fulfil their legal obligations, knowing that most service providers will resort to general monitoring and that several national implementations will most likely require it. Allowing the legislator to abdicate its responsibility to private actors which are in principle not bound by the Charter would leave fundamental rights without effective protection and must therefore be firmly rejected. As the Court highlighted in *UPC Telekabel Wien*:

> *"None the less, when the addressee of an injunction such as that at issue in the main proceedings chooses the measures to be adopted in order to comply with that injunction, he must ensure compliance with the fundamental right of internet users to freedom of information."*[94]

The finding of the Court in the context of an injunction also holds in the context of a legislative obligation. Merely giving a service provider the option to choose the means by which to bring to an end (or prevent) a copyright infringement does not absolve the service provider from

[90] For an analysis of the differences between the content recognition systems voluntarily used by certain platforms today and the requirements of Article 17 (4) CDSMD, see chapter 7.

[91] European Commission, Targeted consultation addressed to the participants to the stakeholder dialogue on Article 17 of the Directive on Copyright in the Digital Single Market, p. 9.

[92] "Besides content recognition technology based on fingerprinting, other solutions, such as watermarking, solutions based on metadata and key word search or a combination of different technologies are currently deployed to detect unauthorised content." Ibid., pp. 8 f.

[93] "Le linee guida della Commissione serviranno a chiarire alcuni di questi punti e si occuperanno anche delle tecnologie applicate per la gestione del copyright, che non vengono menzionate esplicitamente nella direttiva, ma che diventeranno fondamentali per l'applicazione pratica nel riconoscimento dei contenuti. Tali strumenti sono già largamente utilizzati dalla maggiori piattaforme online, sulla base del c.d. fingerprinting." *Viotti*, Copyright, presto legge in Italia la direttiva Ue che fa discutere. https://formiche.net/2020/11/copyright-presto-legge-in-italia-la-direttiva-ue-che-fa-discutere/.

[94] CJEU, C-314/12, ECLI:EU:C:2014:192 – *UPC Telekabel*, para. 55.

choosing a measure that is compliant with users' fundamental rights. In the context of an injunction, the issuing court would be expected to ensure that such measures are indeed available to the service provider. In the context of Article 17 CDSMD, the legislator is required to ensure that all OCSSPs can comply with their legal obligations in a manner that respects the fundamental rights of users.

Even if such alternative means of meeting the requirements of Article 17 CDSMD existed, service providers hoping to avail themselves of those means would be strongly discouraged from implementing them in the light of clear statements from national governments during the legislative process that the use of content recognition technologies is required. When faced with the very tangible risk of payment of damages to rightsholders and even potential criminal liability for copyright infringements, OCSSPs will choose the means of compliance envisioned by the national legislator, even if those requirements may violate users' fundamental rights. As pointed out by Advocate General Saugmandsgaard Øe in his opinion on the *YouTube* and *Cyando* cases:

> *"The risk is that in all these ambiguous situations the provider tends towards systematically removing the information on its servers in order to avoid any risk of liability vis-à-vis the rightholders. It will often find it easier to remove information rather than having to claim itself in the context of a possible action for liability that an exception applies. Such 'over-removal' would pose an obvious problem in terms of freedom of expression."*[95]

While Article 17 (7) CDSMD forbids the removal of illegal content,[96] no sanctions are defined that would compel OCSSPs to respect user rights in situations when the OCSSPs would risk direct liability towards rightsholders if they keep content online that turns out to be infringing. Article 17 CDSMD does not include any rules regarding OCSSPs' liability toward users. It is doubtful whether users would be able to claim any compensation for wrongful removal of content that would dissuade OCSSPs from over-blocking legal content in the future, especially given the difficulty users will face in proving monetary damages in cases that revolve around violations of freedom of expression, rather than economic activities.

Therefore, in order to meet the requirements of the Charter, it is not sufficient for Article 17 CDSMD to state that there is no obligation to monitor, when all available evidence indicates that general monitoring in the form of the use of upload filters will be the sole, or at the very least the dominant, means by which OCSSPs will comply with their obligations under Article 17 CDSMD.

---

[95] Advocate General Saugmandsgaard Øe, Opinion, Joined Cases C-682/18 and C-683/18, ECLI:EU:C:2020:586 – *YouTube* and *Cyando*, para. 189.

[96] This point is disputed among Member States. Seven national governments have written to the European Commission to put forward an interpretation of Article 17 CDSMD that would require platforms to act upon blocking requests of rightsholders without any mechanism to prevent the removal of legal content. Those seven Member State governments seem to interpret Article 17 (7) CDSMD as a mere aspirational statement without operative meaning. Cf. Consultation related to the European Commission's future guidance on the application of article 17 on the Copyright in the digital single market directive, Non paper from Croatia, Denmark, France, Greece, Italy, Portugal and Spain.
https://www.communia-association.org/wp-content/uploads/2020/10/201027non-paper.pdf.

5 Interference of Article 17 with Freedom of Expression and Information

In the EU legislation, the balancing between fundamental rights – such as the right to freedom of expression and the right to intellectual property – takes place during the drafting process of a legislative act. The DSM Directive explicitly references the impact of the Article 17-mechanism on the fundamental rights to freedom of expression and information, notably in recital 70:

> *"The steps taken by online content-sharing service providers in cooperation with rightholders should be without prejudice to the application of exceptions or limitations to copyright, including, in particular, those which guarantee the freedom of expression of users. Users should be allowed to upload and make available content generated by users for the specific purposes of quotation, criticism, review, caricature, parody or pastiche. That is particularly important for the purposes of striking a* ***balance between the fundamental rights*** *laid down in the Charter of Fundamental Rights of the European Union ('the Charter'),* ***in particular the freedom of expression*** *and the freedom of the arts, and the right to property, including intellectual property"* (accentuation by the authors).

In this chapter, we set out why Article 17 CDSMD fails to strike the balance envisioned in recital 70 and therefore violates the freedom of expression and information of the users of OCSSPs. Article 17 CDSMD interferes with the freedom of expression and information of the individual users as well as the general public. It prevents the upload of lawful content that falls under copyright exceptions and limitations, thus restricting the dissemination of content to other users. While Article 17 CDSMD serves the legitimate purpose of protecting the right to intellectual property of rightsholders enshrined in Article 17 (2) CFR, we will show that the proposed mechanism is (i) not proportionate to this aim and (ii) the EU legislator did not comply with its primary obligation to design minimal procedural safeguards for the users' right to freedom of expression and information.

While Poland seeks the annulment of Article 17 (4) points (b) and (c) *in fine* CDSMD on the basis of the violation of the right to freedom of expression and information guaranteed by Article 11 CFR, the considerations below also largely apply to the closely linked fundamental right to freedom of the arts enshrined in Article 13 CFR, given the particular importance of OCSSPs for the sharing of creative expression online.[97]

5.1 Filtering Obligations Interfere with the Users' Freedom of Expression and Information

Article 11 CFR protects two dimensions of the freedom of expression and information: The freedom to impart as well as to receive information. This includes the exchange of information on the internet.[98] According to the CJEU case law, the freedom of expression and information

[97] Advocate General Saugmandsgaard Øe, Opinion, Joined Cases C-682/18 and C-683/18 – *YouTube and Cyando*, ECLI:EU:C:2020:586, para. 241.
[98] CJEU, C-70/10, ECLI:EU:C:2011:771 – *Scarlet,* para. 52.

constitutes one of the fundamental pillars of a democratic society.[99] The freedom of expression and information is not absolute, Article 11 CFR is subject to the general legal reservation of Article 52 (1) CFR. Article 52 (3) CFR further stipulates that the provisions of Article 10 (2) ECHR must be observed in cases of restriction of the freedom of expression and information. From Article 10 (2) ECHR follows that the freedom of expression is subject to certain limitations justified by objectives in the public interest, in so far as those derogations are in accordance with the law, motivated by one or more of the legitimate aims under that provision and necessary in a democratic society, and are, in particular, proportionate to the legitimate aim pursued.[100]

Automatized content filtering leads to potential interferences with the users' freedom of expression and information, a danger that has been voiced by several authors already during the legislative process and is rooted in the CJEU's case law.[101] In the case *SABAM v Netlog*, the CJEU stated that an injunction requiring the implementation of an automated content filtering system:

> *"could potentially undermine freedom of information, since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications".*[102]

Insofar as Article 17 CDSMD requires the implementation of automated filtering systems, this risk applies to the Article 17 liability mechanism. As outlined above, OCSSPs in the scope of the directive will *de facto* be obliged to rely on automated filtering systems at least to some extent in order to avoid liability.[103]

It follows from Article 17 (4)(b) and (c) CDSMD that OCSSPs have to 'filter' unlicensed content and prevent their upload or re-upload, based on the information the rightsholders provide. Although Article 17 (4) CDSMD does not prescribe specific measures to ensure the unavailability of uploaded content, most commentators agree that this requires, at least in some situations, the use of upload filters, i.e. content recognition technologies.[104] In light of the high industry standards for professional diligence required by Article 17 (4)(b) CDSMD, the vast amounts of content that are uploaded, the difficulty to identify content without technical means and the fact that these filtering systems are already being used by some platforms[105], it is clear that Article 17 (4) (b) and (c) CDSMD require automated filtering to analyse and match content that is being uploaded or already present on the platform against the information delivered by rightsholders. Whether or not an OCSSP has fulfilled its obligation

---

[99] CJEU, C-421/07, ECLI:EU:C:2009:222 – *Damgaard,* para. 26.

[100] CJEU, C-71/02, ECLI:EU:C:2004:181 – *Karner,* para. 50; CJEU, C-479/04, ECLI:EU:C:2006:549 – *Laserdisken*, para. 64; CJEU, C-421/07, ECLI:EU:C:2009:222 – *Damgaard,* para. 26.

[101] *See: Quintais*, The New Copyright in the Digital Single Market Directive: A Critical Look, European Intellectual Property Review 2020(1), p 19 with further evidence; *Bridy,* The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform, Vanderbilt Journal of Entertainment & Technology Law, volume 22 (2020), pp. 345 ff.

[102] CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog*, para. 50.

[103] See chapter 2 above.

[104] *Leistner,* European Copyright Licensing and Infringement Liability Under Art. 17 DSM-Directive, ZGE 2020, p 139, *Senftleben,* Bermuda Triangle - Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market, p. 5. https://ssrn.com/abstract=3367219.

[105] For example YouTube's ContentID. https://support.google.com/youtube/answer/2797370?hl1%E2%81%844en-GB.

under Article 17 (4) CDSMD is to be assessed on the basis of high industry standards and in the light of the principle of proportionality provided for by Article 17 (5) CDSMD. In some instances, the principle of proportionality may rule out an obligation to employ filtering systems. However, if automated filtering technology meets industry standards, is most effective, suitable and also not too costly, OCSSPs must use it to fulfil their obligation under Article 17 (4) CDSMD.

5.2 Impact on the Users' Freedom of Expression and Information

To determine whether the interference with Article 11 CFR is proportionate to its legitimate aim, we must first determine how severe the interference with Article 11 CFR is, i.e. to what extent the users' freedom of expression and information is restricted. We argue that the filtering mechanism prescribed by Article 17 (4) CDSMD leads to a significant interference with the users' freedom of expression and information, because the direct liability of OCSSPs (i) incentivizes overblocking and (ii) leads to an ex-ante restriction of the users' freedom of expression and information.

5.2.1 Implication 1: Overblocking of Lawful Content

As mentioned above, the CJEU assessed the impact of automated filtering systems referring to the notion of overblocking. In the cases *Netlog* and *Scarlet*[106], the CJEU pointed out that filtering systems might not distinguish adequately between unlawful content and lawful content, specifically because whether content is lawful depends on the application of statutory exceptions to copyright.[107] In both cases the filtering systems in questions failed to strike a fair balance between the right to intellectual property, on the one hand and – amongst other fundamental rights – the freedom of expression and information on the other.[108]

Collateral overblocking, meaning the over-removal of lawful content, because the content was either falsely blocked for technical reasons or because of overcompliance with copyright laws, is inherent to the context-blindness of filtering systems. State of the art filtering technologies are not suitable to assess the lawfulness of user-generated content. Automated tools are unable to distinguish between lawful and unlawful content, because they cannot judge the context in which content appears.[109] Especially in the field of copyright, context is crucial to determine whether a particular use of a protected work is lawful. Not all uses of copyrighted works are legally actionable, the use of protected material in user-generated content can be lawful under limitations and exceptions to copyright, such as parody or quotation, or on the basis of a license. The identification of a match between an upload and the information provided by a rightsholder is therefore only the first step in determining if the uploaded content infringes copyright laws.

Automated filtering technologies do not go beyond that first step, they are not capable of the complex legal and factual examination that is required to determine if the content falls under

[106] CJEU, C-70/10, ECLI:EU:C:2011:771 – *Scarlet;* CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog*.
[107] CJEU, C-70/10, ECLI:EU:C:2011:771 – *Scarlet,* para. 52; CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog,* para. 50.
[108] CJEU, C-70/10, ECLI:EU:C:2011:771 – *Scarlet,* para. 53; CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog,* para. 51.
[109] *Bridy,* The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform, Vanderbilt Journal of Entertainment & Technology Law, volume 22 (2020), p. 346.

an exception or limitation.[110] The European Commission, after having heard from a variety of stakeholders including the manufacturers of filtering technologies, concluded in its guidance consultation document on the implementation of Article 17 CDSMD that "in the current state of the art, content recognition technology cannot assess whether the uploaded content is infringing or covered by a legitimate use."[111]

This fundamental shortcoming is unlikely to be solved through technological development, as even the most sophisticated filtering technologies that employ machine learning still operate on the basis of recognizing patterns in the data. These tools do not understand the contents of the patterns they detect, hence they are unlikely to perform the qualitative assessments required to determine the presence of humour, or criticism, which are necessary to determine whether a use falls under an exception or limitation. Advanced filtering technologies are capable of making quantitative distinctions regarding the amount of protected material that is used, at least with regard to some types of protected works and other subject-matter. However, these quantitative distinctions fail to align with the legal realities of copyright law. On the one hand, the use of an extremely short extract of a work can constitute an infringement,[112] whereas, on the other hand, the use of an entire work may be permissible, for example in the context of a quotation.

Furthermore, automated filtering systems cannot detect false claims of exclusive rights, including over public domain material or material that is published under a Creative Commons license (overclaiming), nor can they detect whether particular material qualifies for copyright or related rights protection in the first place. The use of automated filtering systems relies entirely upon the veracity of the information provided by presumed rightsholders. The experience with existing automated filtering systems that some large platforms have been using on a voluntary basis has provided empirical evidence for both collateral overblocking and overclaiming by negligent rightsholders.[113] This problem is exacerbated by rightsholders increasingly automating the provision of information about their repertoires to platforms. Those automated schemes are based on the assumption that those rightsholders hold *exclusive* rights in all parts of their repertoires, routinely leading to erroneous requests for the removal of content that is in the public domain or for which rightsholders only hold a non-exclusive usage license.[114]

Insofar as Article 17 (4)(b) and (c) CDSMD require the implementation of automated filtering tools, the danger of overblocking arises. Because of the context-blindness of filtering systems, their implementation will inevitably produce false positives and, through the blocking or removal of lawful content, restrict users' freedom of expression and information. Overblocking constitutes a severe interference with the right to freedom of expression of the affected user whose content is blocked, as well as the right to freedom of information of the

[110] *Bridy,* The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform, Vanderbilt Journal of Entertainment & Technology Law, volume 22 (2020), p. 346.
[111] European Commission, 2020. Targeted consultation addressed to the participants to the stakeholder dialogue on Article 17 of the Directive on Copyright in the Digital Single Market, p. 15.
[112] CJEU, C-476/17, ECLI:EU:C:2019:624 – *Pelham*, para. 29.
[113] *Bridy,* The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform, Vanderbilt Journal of Entertainment & Technology Law, volume 22 (2020), p. 347.
[114] For an example of this phenomenon, German TV station accidentally blocking a political activist group's YouTube video, after having shown it on its TV programme on the basis of a non-exclusive license, see: PinkStinks, RTL hat uns mal kurz gekillt. https://pinkstinks.de/rtl-hat-uns-mal-kurz-gekillt/.

general public, who are denied access to lawful pieces of information. Collateral overblocking amounts to a violation of the freedom of expression because as an unintended effect it does not serve a legitimate aim in itself.[115]

In addition to the direct violation of freedom of expression caused by blocking of lawful content, overblocking also has an indirect negative effect on the freedom of expression of users by causing behavioural changes. These *chilling effects* have been empirically demonstrated in several studies, which showed a drop in individual users' activity on social media platforms after those users had received an automated copyright infringement notice.[116]

Because Article 17 CDSMD imposes a much stricter standard of liability for certain internet service providers, it intensifies the dangers of the over-removal of lawful content. Outside the scope of the CDSMD, the liability of internet service providers is not harmonized. According to Article 14 of the E-Commerce Directive (ECD), hosting services that store third-party content cannot be held liable for illegal acts of their users unless they obtained actual knowledge about the illegality of a piece of illegal information (notice) and failed to act expeditiously to avoid liability (takedown). The ECD itself does, in contrast to Article 17 CDSMD, does not impose direct liability on intermediaries. Within the framework of the ECD, the design of the obligations of hosting service providers is therefore left to the Member States, to the extent that the national laws respect the liability limitation provided for in Article 14 ECD. For a subset of hosting service providers, the OCSSPs, this liability framework changes significantly with the adoption of Article 17 CDSMD.[117]

5.2.2 Implication 2: Ex-ante Restrictions of the Freedom of Expression and Information

While the mere fact that Article 17 (4)(b) and (c) CDSMD require to some extent the use of algorithmic filtering tools may seem to be a technical matter, it reflects a fundamental shift in the balance of copyright law. The possibility of ex-ante automated blocking or removal of content reverses the default treatment of potentially legal content:

> *"if copyrighted materials were once available unless proven to be infringing, today materials that are detected by algorithms are removed from public circulation unless explicitly authorized by the right holder."*[118]

The interference with fundamental rights is especially severe because it leads to an ex-ante restriction of the users' freedom of expression and information. Potentially lawful content can be blocked or removed before a court or independent judicial body has assessed its lawfulness. Poland argues in this plea that this shift in the balance of copyright enforcement caused by the mandatory introduction of automated filtering systems undermines the

[115] *Husovec*, Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p. 5.
[116] Cf. *Matias et al.*, Do Automated Legal Threats Reduce Freedom of Expression Online? Preliminary Results from a Natural Experiment. https://osf.io/nc7e2/; *Penney*, Privacy and Legal Automation: The DMCA as a Case Study. 22 Stan. Tech. L. Rev. 412. https://www-cdn.law.stanford.edu/wp-content/uploads/2019/09/Penney_20190923_Clean.pdf.
[117] *Husovec*, Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p. 3.
[118] Elkin-Koren, *Fair Use by Design*, UCLA Law Review 64 (2017), p. 1093.

essence of the fundamental rights to freedom of expression and information, because it can cause information to be prevented from publication altogether,[119] rather than being initially made available and blocked at a later point, once its illegality has been determined. Insofar as automatic filtering systems are implemented to fulfil the obligations according to Article 17 (4) CDSMD, potentially lawful content will to some extent be initially blocked and can only be published after having undergone a complaint and redress procedure – without ever involving an independent body to assess its lawfulness.

5.2.3 CJEU Case Law on Overblocking and ex-ante Restrictions of Freedom of Expression and Information

The case law of the CJEU provides some guidance regarding the impacts of overblocking and ex-ante restrictions on Article 11 CFR. In the above-mentioned cases *Netlog* and *Scarlet*[120] the CJEU ruled that injunctions requiring the installation of the contested content filtering systems were inadmissible. In his opinion on the case *Scarlet*, AG Villalón went so far to conclude that

> '*no filtering and blocking system appears able to guarantee, in a manner compatible with the requirements of Articles 11 and 52 (1) of the Charter, the blockage only of exchanges specifically identifiable as unlawful*'. [121]

The decisions in *Netlog* and *Scarlet* were followed by a number of other judgements that all support the interpretation that overblocking is a priori incompatible with the right to freedom of expression and information. Some authors conclude from the decision of the CJEU in *UPC Telekabel*[122] that the effects of Article 17 CDSMD regarding the implementation of filtering mechanisms might be proportionate.[123] However, the ruling in the case *UPC Telekabel* actually supports the opposite conclusion, by strictly rejecting the permissibility of overblocking. In its ruling the CJEU approved an injunction that required internet access providers to block access to a particular website offering access to infringing content only under the condition that the measures employed by the service provider to comply with the injunction are effective, "without thereby affecting internet users who are using the provider's services in order to lawfully access information".[124]

The CJEU's decision nevertheless raised fundamental rights questions, because it did not "specify the measures which that access provider must take" and insofar delegating the responsibility to strike a balance between the competing fundamental rights of rightsholders and users to the addressee of the injunction.[125] This criticism does not, however, relate to the dangers of overblocking. Because the injunction in question was strictly targeted at a particular website whose contents were pre-determined to consist of materials made available exclusively or predominantly without the rightsholder's consent,[126] there is no risk

[119] This issue is discussed in detail below in light of the ECtHR case-law regarding prior restraint.
[120] CJEU, C-70/10, ECLI:EU:C:2011:771 – *Scarlet;* CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog*.
[121] AG Villalón, Opinion, C-70/10, ECLI:EU:C:2011:255 – *Scarlet*, para. 86.
[122] CJEU, C-314/12, ECLI:EU:C:2014:192 – *UPC Telekabel*.
[123] *Specht-Riemenschneider,* Leitlinien zur Umsetzung des Article17 DSM-RL aus Verbrauchersicht, p. 47. https://www.vzbv.de/sites/default/files/downloads/2020/06/23/2020-06-12-specht-final-art_17.pdf.
[124] CJEU, C-314/12, ECLI:EU:C:2014:192 – *UPC Telekabel*, para. 56.
[125] CJEU, C-314/12, ECLI:EU:C:2014:192 – *UPC Telekabel,* para. 64.
[126] Ibid., para. 3.

of blocking lawful communications comparable to that resulting from the implementation of a content filtering system required by Article 17 (4) CDSMD.

Also, the CJEU's decision in the case *Glawischnig-Piesczek*[127] does not lend support to the legality of overblocking, although this time it involved an injunction that required a social network to monitor all content for identical and equivalent defamatory statements uploaded by users. In the decision *Glawischnig-Piesczek* the Court avoids the balancing of fundamental rights despite the fact that AG Szpunar mentions that the injunction in question must respect the internet users' fundamental rights to freedom of expression and information, irrespective of their lack of standing in the court proceedings.[128] Instead, the Court deems injunctions to be permissible only insofar as they concern the blocking of statements that are either identical to the defamatory statement deemed illegal by the referring court, or equivalent statements that the court has *listed* in the injunction and therefore deemed to be equally illegal. "Differences in the wording of that equivalent content, compared with the content which was declared to be illegal, must not, in any event, be such as to require the host provider concerned to carry out an independent assessment of that content."[129] While this ruling fails to give much guidance on how these requirements can be met in practice, given the context-sensitivity of defamation, it does not give support to an injunction that would lead to the blocking of legal content as collateral damage.

Following these decisions, the danger of overblocking can be said to inform the CJEU's decision in judging whether a specific filtering system strikes a fair balance between the fundamental right to property, and the fundamental right to freedom of expression and information. The CJEU places importance on the requirement that blocking injunctions do not lead to the blocking of lawful content. It is that requirement which saw the CJEU judging that the blocking injunctions requiring the implementation of automated filtering systems in the copyright context were incompatible with EU law.

5.2.4 ECtHR Case Law on Overblocking and ex-ante Restrictions of Freedom of Expression and Information

The meaning and the scope of the fundamental right to freedom of expression within the EU legal order can be further clarified by the ECtHR case law. Article 52 (3) CFR states that insofar as rights of the Charter correspond to rights which are guaranteed by the ECHR, the meaning and scope of those rights shall be the same. This applies not only to the wording of the ECHR, scope and meaning of the provisions of the Charter are also to be determined by the ECtHR case law on the corresponding provisions.[130]

The ECtHR has an extensive case law on the impacts of website blocking on the freedom of expression. In determining the severity of the interference with the freedom of expression, the ECtHR notes that overblocking constitutes a type of prior restraint, because an information is blocked before a judicial decision on the lawfulness of the content was

[127] CJEU, C-18/18, ECLI:EU:C:2019:821 – *Glawischnig-Piesczek.*
[128] AG Szpunar, Opinion, C-18/18, ECLI:EU:C:2019:458 – *Glawischnig-Piesczek*, para. 65.
[129] CJEU, C-18/18, ECLI:EU:C:2019:821 – *Glawischnig-Piesczek*, para. 45.
[130] CJEU, C-205/15, ECLI:EU:C:2016:499 – *Toma und Biroul Executorului Judecătoresc Horațiu-Vasile Cruduleci,* para. 41.

issued.[131] The Court reiterates in this connection that prior restraints are not prohibited by Article 10 ECHR as such, but the dangers inherent in prior restraints '*call for the most careful scrutiny on the part of the Court and are justified only in exceptional circumstances'.*[132] This is especially relevant when the access to information on the internet is restricted, as:

> *"in the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general."*[133]

The Court adds that preventive restrictions on the freedom of expression and information require a legal framework establishing precise and specific rules regarding the application of preventive restrictions.[134] The ECtHR's case law makes it therefore clear that ex-ante restrictions of the freedom of expression constitute an especially severe interference that can only be justified in exceptional circumstances.

In *Ahmet Yildirim v Turkey*, the ECtHR also addressed the issue of collateral overblocking. The Court ruled that the injunction in question violated Article 10 ECHR, because it led to a significant collateral blocking of lawful websites.[135] The ECtHR in *Kharitonov v Russia*[136] ruled that the Russian website blocking scheme that led to blocking of websites that shared the same IP address was a violation of Article 10 ECHR because it led to arbitrary and excessive blocking of lawful websites. The Court argues that any measure that renders large quantities of information inaccessible substantially restricts the rights of Internet users. Whenever a measure interferes with lawful content or websites as a collateral effect, the legal framework must establish safeguards capable of protecting individuals from excessive and arbitrary effects of blocking measures. When exceptional circumstances justify the blocking of unlawful content,

> *"a State agency making the blocking order must ensure that the measure strictly targets the illegal content and has no arbitrary or excessive effects, irrespective of the manner of its implementation*".[137]

The ECtHR has so far not approved of a single blocking system. [138] Even in hate speech cases, where the ECtHR gives the Member States greater latitude, it did not approve of pre-publication restraints.[139] The ECtHR case law on blocking systems shows that the Court regards ex-ante restrictions of the right to freedom of expression and information as an especially severe interference. This interference can only be justified in exceptional circumstances and

---

[131] ECtHR, Applications nos. 48310/16 and 59663/17 – *Kablis v. Russia*, para. 90.
[132] ECtHR, Application no. 3111/10 – *Ahmet Yildirim v Turkey,* para. 47.
[133] ECtHR, Application no. 3111/10 – *Ahmet Yildirim v Turkey,* para. 48.
[134] ECtHR, Applications nos. 48310/16 and 59663/17 – *Kablis v. Russia*, para. 92.
[135] ECtHR, Application no. 3111/10 – *Ahmet Yildirim v Turkey,* paras. 66–68.
[136] ECtHR, Application no. 10795/14 – *Kharitonov v Russia*.
[137] ECtHR, Application no. 10795/14 – *Kharitonov v Russia*, paras. 45 f.
[138] *Husovec,* Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible?, Forthcoming, p. 10.
[139] In *Delfi AS v. Estonia,* Application no. 64569/09 – *Delfi AS v. Estonia*, the ECtHR accepted that states may impose liability if the portals fail to remove certain kinds of hate speech, however, *Delfi AS v Estonia* only referred to certain kinds of hate speech for which the ECtHR accepted ex-post removal (para. 159), and did not approve of preventive filtering of content before its publication.

require a precise and specific legal framework. Even if an ex-ante restriction is justified to block unlawful content, the Court clearly spells out that this must not lead to overblocking.

Although the ECtHR's cases dealt with the blocking of websites, the same analysis applies to service providers hosting user-generated content. In *Kablis v Russia,* the ECtHR confirmed that the blocking of individual content falls under the same category of interferences, that is prior restraints, because it amounts to a limitation of the freedom of expression and information prior to judicial determination of lawfulness.[140]

5.3 Conclusion: Article 17 Results in Serious Interference with Freedom of Expression and Information

In conclusion, the interference with the freedom of opinion which Article 17 CDSMD causes is of particular severity under European law. The blocking of content before its publication and before a court has assessed its lawfulness is a prior restraint according to the ECtHR's case law that can only be justified in exceptional circumstances. Both the CJEU and the ECtHR place great importance on the fact that filtering systems may lead to the collateral overblocking of lawful content.

Both courts regard the collateral blocking of lawful content as a severe interference with the users' fundamental right to freedom of expression and information. They have found that filtering or blocking systems that lead to arbitrary blocking of lawful content violate Article 11 CFR and Article 10 ECHR respectively. In the application and interpretation of Article 11 CFR by the CJEU, the ECtHR's case law can provide further guidance. It follows from Article 52 (3) CFR that the CJEU must also take the relevant ECtHR case law into account when interpreting the Charter. In the ECtHR's case law on website blocking, it is well established that ex-ante restrictions of the freedom of expression and information on the internet can only be justified in exceptional circumstances and require a precise and specific legal framework. As will be shown below, Article 17 CDSMD fails to meet this standard.

6 Insufficient Safeguards for Freedom of Expression and Information

As a result of the highly charged political process, several statutory provisions adding mandatory exceptions and safeguards against the blocking of lawful content were implemented into the directive at a late stage of the legislative process. The co-legislators expressly introduced these procedural safeguards as means to mitigate the impact of the Article 17-mechanism on the freedom of expression and information of users.

In the following, we explain why Article17 CDSMD does not contain sufficient procedural safeguards to mitigate the interference with the users' fundamental right to freedom of expression and information that we described above. To this end, we will first present the requirements for procedural safeguards arising from primary Union law and the case law of CJEU and ECtHR and show that the safeguards foreseen in Article 17 CDSMD do not compensate the impact on the users' freedom of expression and information, also because the EU legislator failed to lay down sufficient minimal procedural safeguards.

[140] ECtHR, Applications nos. 48310/16 and 59663/17 – *Kablis v. Russia*, para. 90.

6.1 European Case Law Requires Minimal Procedural Safeguards

To determine to what extent the safeguards enshrined in Article 17 CDSMD can mitigate the interference with users' freedom of expression and information, we briefly analyse the criteria for procedural safeguards which the CJEU establishes in its case law on filter systems as well as the relevant case law of the ECtHR.

6.1.1 CJEU Case Law on Filtering Systems and Procedural Safeguards

The CJEU's case law on filter systems does not contain clear guidelines on procedural safeguards for the fundamental rights of the users. In the decisions already discussed above, *UPC Telekabel* and *Glawischnig-Piesczek*, the CJEU develops, at best, indications of procedural safeguards against interferences with the users' fundamental rights due to overblocking.[141]

In *UPC Telekabel*, the CJEU approved an injunction that required internet access providers to block particular websites but did not *"specify the measures which that access provider must take"*.[142] The court held that access providers themselves must be required by national laws to "ensure compliance with the fundamental rights of internet users to freedom of information" by adopting measures that "*bring an end"* to the specified infringement *"without thereby affecting internet users who are using the provider's services in order to lawfully access information".* To avoid conflicts with fundamental rights, the CJEU adds that *"the national procedural rules must provide a possibility for internet users to assert their rights before the court once the implementing measures taken by the internet service provider are known*".[143]

In *Glawischnig-Piesczek*, the CJEU did not examine this precedent but concluded that a court order that requires a social network to monitor all uploaded content so long as the monitoring is "*limited to information containing the elements specified in the injunction, and its defamatory content of an equivalent nature does not require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies."*[144] The Court did neither mention nor expand on the requirement of procedural safeguards established in *UPC Telekabel*. This ultimately leads to the fact that the protection of the fundamental rights of users is entirely placed in the responsibility of the court issuing the order. The injunction itself has to *"properly identify"* the infringing nature and contain specific elements, including its context.[145]

These decisions show that the CJEU guidelines on procedural safeguards against the dangers of overblocking are rudimentary.[146] This may be related to the fact that the CJEU delegates the responsibility to protect the fundamental rights of users to other actors. In *UPC Telekabel*,

---

[141] *Husovec,* Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p. 9.
[142] CJEU, C-314/12, ECLI:EU:C:2014:192 – *UPC Telekabel,* para. 64.
[143] CJEU, C-314/12, ECLI:EU:C:2014:192 – *UPC Telekabel,* para. 57.
[144] CJEU, C-18/18, ECLI:EU:C:2019:821 – *Glawischnig-Piesczek,* paras. 46–47.
[145] CJEU, C-18/18, ECLI:EU:C:2019:821 – *Glawischnig-Piesczek,* para. 45.
[146] It should already be emphasized at this point that the above-mentioned decisions differ from the constellation in Poland v European Parliament and Council. We will show below that for the subject matter of the case, the European legislator is obliged to provide safeguards based on the current interpretation of the legal framework.

it is the access providers who have to safeguard the rights of users. In *Glawischnig-Piesczek*, it is the national courts who have the hard-to-follow task of describing an infringement so precisely that service providers can detect it using automatic tools without blocking legitimate uses of the same content in other contexts.

6.1.2 ECtHR Case Law on Filtering Systems and Procedural Safeguards

Again, the ECtHRs case law on website blocking and the impacts on the freedom of expression and information provides substantial guidance that the CJEU can rely on in its interpretation and application of Article 11 CFR.[147]

The far-reaching delegation of responsibilities is in contrast to the case law of the ECtHR on the interferences of website blocking schemes with the freedom of expression and information. As outlined above, the ECtHR has ruled on the admissibility of website blocking schemes in various cases and has not yet accepted a single blocking system. All of the ECtHR's case law finds violations of the freedom of expression and information due to insufficient safeguards. The starting point in all these cases is that the blocking of content before its unlawfulness has been established is a type of prior restraint.[148]

The ECtHR explicitly states that "a legal framework is required to ensure both tight control over the scope of bans and an effective Convention-compliant judicial review".[149] According to the ECtHR, legislation must "provide safeguards against abuse (...) in respect of incidental blocking measures".[150] Legislation that leads to preventive restrictions of the fundamental right to freedom of expression and information must itself contain a precise and specific framework regarding the application of these restrictions.[151]

In the decisions of *Kharitonov v Russia, OOO Flavus v Russia and Engels v Russia*, the ECtHR found that website blocking schemes violated Article 10 ECHR for not including the following safeguards: (i) an impact assessment of the blocking measure prior to its implementation, (ii) an obligation to proactively notify and educate those who might be impacted by overblocking, (iii) the blocking measures had not been sanctioned by a court or other independent adjucatory body, (iv) they lacked effective transparency with respect to grounds and possibilities to challenge already implemented blocking measures, (v) and did not provide for judicial recourse for the parties.[152]

6.2 EU Legislator Has Central Responsibility to Provide Minimal Safeguards

What are the practical implications for Article 17 CDSMD that can be derived from these standards of the European case law?

---

[147] CJEU, C-205/15, ECLI:EU:C:2016:499 – *Toma und Biroul Executorului Judecătoresc Horațiu-Vasile Cruduleci,* para. 41.
[148] *Husovec*, Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p. 10; ECtHR, Application no. 10795/14 – *Kharitonov v Russia*, para. 43.
[149] ECtHR, Application no. 3111/10 – *Ahmet Yildirim v Turkey* para. 64.
[150] ECtHR, Application no. 10795/14 – *Kharitonov v Russia*, para. 43.
[151] ECtHR, Applications nos. 48310/16 and 59663/17 – *Kablis v. Russia*, para. 92.
[152] *Husovec,* Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p 10; ECtHR, Application no. 10795/14 – *Kharitonov v Russia*, paras. 43–45, 55.

At the outset, we have shown that the Article 17 CDSMD-mechanism leads to severe interference with the users' freedom of expression and information, because it imposes preventive restrictions and may lead to the over-removal of lawful content. This corresponds to the balancing of interests underlying the ECtHR's case law on website blocking.[153] As a result of the severity of interference, the minimal requirements to be set for the safeguards are strict. However, the subject matter of the decisions cited above differs from the case *Poland v European Parliament and Council*. In the present case, it is not a matter of a court order, but of obligations imposed upon service providers by statutory provisions, namely the Directive itself. Since a directive necessarily leaves the Member States some leeway for implementation, the question is what minimal procedural safeguards the EU legislator must itself take and lay down in the directive.

6.2.1 EU Legislator Must Balance Fundamental Rights in Directives

The underlying principle is that the European legislator is bound by the fundamental rights of the CFR according to Article 51 (1) CFR. The obligation to respect fundamental rights sets limits to the imposition of measures by the EU legislator on service providers where those measures are associated with an interference with the fundamental rights of service providers and users. Primarily, the European legislator itself must ensure that the directive is designed in conformity with fundamental rights. In her Opinion on the case *Promusicae*, AG Kokott concludes that *"[t]he balance between the relevant fundamental rights must first be struck by the Community legislature*".[154]

Secondarily, when implementing a directive, Member States are obliged to observe the CFR, "*when using up any remaining margin for regulation in the implementation of directives*".[155] Or, as the CJEU puts it, when implementing a directive, "*Member States must [...] take care to rely on an interpretation of the directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order*".[156] This means that drafting a directive in such a way that it can be implemented in accordance with fundamental rights remains the responsibility of the EU legislator.

It is therefore primarily the responsibility of European legislator to ensure that a directive be implemented in conformity with the CFR. The more serious the threats to fundamental rights posed by the respective provisions, the narrower the specifications must be.[157] A central element in ensuring this is the design of procedural safeguards. The protection of fundamental rights by means of procedural safeguards has so far played a central role in decisions on the admissibility of data protection laws, before national constitutional courts[158] as well as before

[153] ECtHR, Applications nos. 48310/16 and 59663/17 – *Kablis v. Russia*, para. 90.
[154] Advocate General Kokott, Opinion, C-275/06, ECLI:EU:C:2007:454– *Promusicae*, para. 56.
[155] Ibid.
[156] CJEU, C-275/06, ECLI:EU:C:2008:54 – *Promusicae*, para. 68.
[157] *Husovec*, Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p 14. See also CJEU, C-293/12 and C-594/12, ECLI:EU:C:2014:238 – Digital Rights Ireland Ltd, para. 55.
[158] BVerfG [German Constitutional Court], Case No. 1 BvR 256, 263, 586/08.

the CJEU[159]. Most recently it also led to the French AVIA law being annulled by the Conseil Constitutionell.[160]

6.2.2 CJEU Spells Out Clear Requirements – *Digital Rights Ireland* and *Schrems II*

In its decision[161] on the Data Retention Directive, the CJEU recognised that the European legislator has the primary (in the words of Martin Husovec 'central') responsibility to design minimal safeguards in legislative acts that affects the fundamental rights of EU citizens.[162]

The CJEU considered the procedural safeguards of the Data Retention Directive to be insufficient to protect the fundamental rights of data subjects. With reference to the case law of the ECtHR, the CJEU held that

> *"**the EU legislation** in question **must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimal safeguards** so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where (…) personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data" (accentuation by the authors).* [163]

The CJEU thus took up the argumentation of AG Villalón, who argued in his opinion in *Digital Rights Ireland* that:

> "*The European Union legislature cannot, when adopting an act imposing obligations which constitute serious interference with the fundamental rights of citizens of the Union, entirely leave to the Member States the task of defining the guarantees capable of justifying that interference. It cannot content itself either with assigning the task of defining and establishing those guarantees to the competent legislative and/or administrative authorities of the Member States called upon, where appropriate, to adopt national measures implementing such an act or with relying entirely on the judicial authorities responsible for reviewing its practical application. It must, if it is not to render the provisions of Article 51(1) of the Charter meaningless, fully assume its share of responsibility by defining at the very least the principles which must govern the definition, establishment, application and review of observance of those guarantees."*[164]

In its recent decision in the case *Schrems II*[165], the CJEU confirmed that the "*legal basis which permits the interference with [fundamental] rights must itself define the scope of the limitation*

---

[159] As shown below CJEU, C-293/12 and C-594/12, ECLI:EU:C:2014:238 – *Digital Rights Ireland Ltd.*
[160] Conseil Constitutionnel, Décision n° 2020-801 DC du 18 juin 2020.
[161] CJEU, C-293/12 and C-594/12, ECLI:EU:C:2014:238 – *Digital Rights Ireland Ltd*.
[162] *Husovec*, Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p. 12.
[163] CJEU, C-293/12 and C-594/12, ECLI:EU:C:2014:238 – *Digital Rights Ireland Ltd*, para. 54.
[164] AG Villalón, Opinion, C-293/12 and C-594/12, ECLI:EU:C:2013:845– *Digital Rights Ireland Ltd*, para. 120.
[165] CJEU, C-311/18, ECLI:EU:C:2020:559 – *Schrems II*.

on the exercise of the right concerned"; and reiterated the requirement of clear and precise rules, including minimal safeguards in order to satisfy the requirement of proportionality.[166]

The CJEU thereby lays down two central requirements for the design of directives: the directive itself must provide a minimal degree of procedural safeguards. The requirements for these safeguards are all the stricter the greater the potential threat to the fundamental rights of the persons concerned. The CJEU herewith expressly confirms the division of responsibilities between the European legislator and the Member States as outlined by AG Kokott in the *Promusicae* case. If the European legislator limits the fundamental rights by means of legislative acts, it must also ensure that any implementation by the Member States is in accordance with the Charter. A directive does not have to define exhaustively all the safeguards. However, the stronger the intervention in fundamental rights in the directive, the narrower the specifications must be.[167]

Considering these requirements, it is not sufficient, that Member States have a possibility to interpret a Directive in a conformant way. A rather conservative approach assumes that a directive can only be annulled under the condition that any conceivable implementation would lead to an unjustified impairment of fundamental rights guarantees.[168] Taking into account the importance of the legislator's responsibility for the rule of law[169] this point of view is not convincing. The EU legislator cannot have the option to divorce the issue of safeguards for strategic reasons, at the expense of EU citizens and their rights. Especially when dealing with a controversial topic like the one at hand, this would lead to a reopening of the debate on central issues at the national level. This does not do any justice to the character of the Directive as an instrument of harmonization. Moreover, this understanding is also in line with the approach of the CJEU in the Digital Rights Ireland case. Considering amongst others the legislators' failure to impose safeguards, the CJEU deemed the directive to be incompatible with the principle of proportionality.[170] Therefore, the directive was invalid. This judgment can be transposed to the case *Poland v European Parliament and Council*.

In addition, the fact that the lack of safeguards is linked to the inconsistency and ambiguity of the substantive requirements also speaks for the necessity of this approach. As a result of this way of operating, the legislator practically misses the goal of harmonization through the directive.

6.3 Conclusion: Article 17 CDSMD Does not Sufficiently Safeguard the Freedom of Expression and Information

[166] Ibid., paras. 175 f.
[167] *Husovec*, Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p. 14.
[168] *Peters/Schmidt,* Das Ringen um Upload-Filter geht in die 2. Runde, GRUR Int 2019, p 1019. De facto also *Leistner,* European Copyright Licensing and Infringement Liability Under Art. 17 DSM-Directive, ZGE 2020, fn. 53, 88. In the same direction also *Specht-Riemenschneider,* Die Entwicklung des IT-Rechts im Jahr 2019, NJW 2019, p 3688. *Husovec*, Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p. 18, considers it to be more likely that the CJEU will give broader deference to the EU legislator, but does not explicitly state an own opinion.
[169] See *Husovec*, Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p. 18.
[170] CJEU, C-293/12 and C-594/12 ECLI:EU:C:2014:238 – *Digital Rights Ireland Ltd*, para. 69.

Ultimately, the safeguards in Article 17 CDSMD do not meet the strict requirements of EU law.[171] An analysis of the safeguards foreseen in Article 17 CDSMD shows that the EU legislator did not fulfil its central responsibility to design clear and precise provisions to safeguard the users' fundamental rights to freedom of expression and information.

In particular, Article 17 CDSMD contains the following mechanisms:[172]

a. the necessity of complaint and redress mechanism for users in the event of disputes (Article 17 (9) CDSMD);
b. the need for a justification of rightsholders' requests and the timely processing of complaints through humans (Article17 (9) CDSMD);
c. the necessity of out-of-court redress mechanisms as well as efficient judicial remedies (Article 17 (9) CDSMD);
d. the rendering obligatory of certain exceptions and limitations that are central to the protection of freedom of expression (Article 17 (7) CDSMD),
e. The relevance of the principle of proportionality for the determination of the obligations under Article17 (4) CDSMD and the flexibility of the obligations (Article17 (5) CDSMD);
f. the goal that the application of the provision shall not restrict access to the content uploaded by users which do not infringe copyright or related rights and shall not otherwise affect legitimate uses (Article17 (7) and (9) CDSMD),
g. the requirement that the provision may not lead to any general monitoring obligation (Article 17 (8) CDSMD) and
h. the necessity of compliance with data protection legislation (Article17(9) CDSMD).

These safeguards can be divided into two different categories: specific safeguards and general safeguards. Whereas the first group of safeguards concern specific acts of the persons involved – i.e. rightsholders, platforms, or users –, the latter one deals with the functionalities of the OCSSPs in a broader sense.

Specific safeguards are the internal and external complaint and redress mechanisms described in Article 17 (9) CDSMD. These are the mechanisms described above under lit. a. to d. When looking at these safeguards, it is noticeable that they refer only to ex-post recourse. The specifically prescribed recourse mechanisms only come into play once a potentially legal upload has already been blocked. This reflects the fundamental tilt in the balance of copyright enforcement that is brought about by the Article 17-mechanism: (Potentially) lawful content can automatically be blocked upon a rightsholder's request.[173] On a granular level, it reflects the dangers of overblocking that follow the implementation of the Article 17-mechanism. As was already stated, the very existence of these mechanisms shows that the EU legislator was

[171] With the same result *Husovec,* Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p. 16.
[172] *Husovec,* Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, pp. 15 f.
[173] *Schwemer/Shovsbo*, What is Left of User Rights? Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime, Forthcoming in Paul Torremans (ed.), Intellectual Property Law and Human Rights, 4th edition, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3507542. With an empirical assessment to overblocking *Urban et al.,* 'Takedown in Two Worlds: An Empirical Analysis', (2018) 64 JCS 483; *Elkin-Koren/Bar-Ziv,* Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice and Takedown, (2017) 50(2) CLR.

aware that Article 17 CDSMD will lead to situations where OCSSPs falsely take down lawful content. Also, the in-platform complaint and redress mechanism bears a risk of over-enforcement in order to avoid the strict liability under Article 17 CDSMD. OCSSPs are likely to act cautiously regarding the interpretation of copyright exceptions, as the final decision by an OCSSP to reinstate content whose legal status is unclear exposes the OCSSP to possible liability.[174] This intensifies the risk of overblocking.[175] The obligation on Member States to make certain copyright exceptions and limitations mandatory under lit. d falls into this category, because it merely affects the question whether certain user uploads violate copyright law and may thereby affect the outcome of the redress mechanism, but this safeguard does not in and of itself provide any mechanism to ensure that these uploads will not be blocked to begin with.

Besides the specific safeguards, Article17 CDSMD also includes general safeguards (lit. e. to h.). Each of those safeguards can be criticized with good reasons: It is not clear which practical implications shall derive form the requirement of Article 17 (5) CDSMD, that the obligations after Article17 (4) CDSMD have to be determined in light of the principle of proportionality. The provision itself as well as the recitals missed out on the opportunity to give further guidance on how this provision is to be interpreted.[176] OCSSPs will be incentivised to over-comply in the absence of guidance on whether particular measures are sufficient to evade strict liability.

Article 17 (7) CDSMD stipulates that the cooperation between OCSSPs and rightsholders:

> *"shall not result in the prevention of the availability of works (…) uploaded by users, which do not infringe copyright and related rights, including where such works or other subject matter are covered by an exception or limitation".*

As has already been pointed out with regard to the structure of Article17 CDSMD, the goal set out in paragraph 7 stands in inherent contradiction to the liability system itself. It is not clear which measures must be taken by whom in order to fulfil the substantive requirement of the provision. Member States are left alone with this dilemma. It is therefore not surprising that Member States have apparent difficulties to implement tangible provisions to meet the requirements of the rather abstract provision, leading a significant number of Member States to conclude that Article 17 (7) CDSMD does not require them to implement any ex-ante protections against the blocking of legitimate content whatsoever[177] and others intending to transpose this provision verbatim[178]. Article 17 (7) CDSMD clearly fails to meet the

[174] *Senftleben,* Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market, p. 9. https://ssrn.com/abstract=3367219.
[175] *Schwemer/Shovsbo*, What is Left of User Rights? Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime, Forthcoming in Paul Torremans (ed), Intellectual Property Law and Human Rights, 4th edition, 2020, p. 13. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3507542.
[176] *Samuelson* Pushing Back on Stricter Copyright ISP Liability Rules, Michigan Technology Law Review, Forthcoming, p. 13. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3630700.
[177] Consultation related to the European Commission's future guidance on the application of article 17 on the Copyright in the digital single market directive. Non paper from Croatia, Denmark, France, Greece, Italy, Portugal and Spain.
https://www.communia-association.org/wp-content/uploads/2020/10/201027non-paper.pdf.
[178] For an overview of Member States' implementation proposals, see Communia Association. DSM Directive Implementation Tracker.
https://www.notion.so/DSM-Directive-Implementation-Tracker-361cfae48e814440b353b32692bba879.

requirement formulated by AG Villalón that EU law govern the application and review of observance of fundamental rights guarantees,[179] given that it is entirely left open how this provision is to be enforced.

At last, according to Article 17 (8) CDSMD, the application of the Article 17-mechanism shall not lead to any general monitoring obligation. As explained in chapter 3, it is not possible for an OCSSP to act in accordance with Article17 (4) (b) and (c) CDSMD without violating this prohibition.

Against this background, the EU legislator did not assume its primary responsibility to lay down clear and precise minimal procedural safeguards. With regard to the 'specific' safeguards, the Directive leaves the design of the complaint and redress mechanisms entirely to the Member States. The text of the Directive does not provide for basic information rights of users, nor for state oversight or transparency.

In addition, the directive contains no provisions on how Member States should ensure that the decisions of the in-platform redress mechanisms are effectively enforced. In particular, it fails to ensure that OCSSPs cannot evade their obligations toward users by resorting to the blocking of user uploads on the basis of their terms and conditions, rather than on the basis of Article 17 CDSMD.[180] Together with the lack of transparency, it can therefore neither be guaranteed nor verified whether and how OCSSPs actually implement a decision.[181] The in-platform redress mechanism is in itself not sufficiently safeguarded. Although the Directive stipulates that the redress mechanism has to be effective, expeditious, involve a human review, EU law foresees no oversight or sanctions, nor is there a reference to a need for such measures in the implementation of the directive.[182]

The general safeguards are not suitable to mitigate the interferences with the fundamental rights of users. They do not provide '*sufficient guarantees to effectively protect*' their rights from the prior restraint imposed by the Article 17-mechanism. The only ex-ante protection for the users' fundamental rights is laid down in general provisions that lack concretization and enforceability. This blind spot of the directive is especially problematic given the fact that it may be economically advantageous for platforms to over-comply with their obligations under Article 17 (4) CDSMD. Against this background, the provisions fail to properly mitigate the risks for users' fundamental rights.

Article 17 (7) and (8) CDSMD describe an outcome, without giving indications how this outcome can be achieved. This leads to the irreconcilable contradictions described in chapter 2. It is far from clear how users are supposed to enforce their rights under the Directive. The Directive does not specify any consequences for platforms who fail to ensure that no legal

[179] AG Villalón, Opinion, C-293/12 and C-594/12 ECLI:EU:C:2013:845 – *Digital Rights Ireland Ltd,* para. 120.
[180] The experience with the German Network Enforcement Act shows that this is not merely a theoretical concern. Cf. *Wagner et al.*. Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act, FAT 2020.
[181] *Husovec,* Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p. 15.
[182] Ibid. p. 17.

content is removed; Article17 CDSMD does not foresee that providers would face any sanction for not respecting the proportionality of preventive duties.[183]

Article 17 CDSMD does not provide the users with the possibility to challenge the legitimacy of the filtering system implemented under Article 17 (4) CDSMD as such. The redress mechanisms are confined to specific instances of unjustified removal of lawful content.[184] Users therefore have to rely on the ex-post redress mechanism that is not sufficient to safeguard the freedom of expression and information on the Internet. If a lawful criticism or parody can only be made public after having undergone a complaint and redress procedure, the decisive moment for the affected quotation or parody may already have passed.[185] Especially in the context of political speech, a delay in the exercise of the fundamental right to freedom of expression and information can be tantamount to a prevention of the exercise of that right.

Apart from the time aspect, complaint systems may also be implemented in a way that discourages widespread use.[186] Again, users have no possibility to challenge these general deficiencies in court. Yet in *UPC Telekabel*, the CJEU considered that in a similar situation of an open-ended injunction, the affected users must be able to assert their rights under the Charter before a national court.[187] Those rights include the freedom of expression and information, from which the requirement of a strict targeting is deduced. Article 17 (9) CDSMD, on the other hand, only confers upon users the right to assert the use of an exception or limitation in court, but not the right to challenge the functioning of the mechanism that governs whether uses that fall under an exception or limitation are blocked in the first place. The impact on the fundamental rights seems considerably lower in *UPC Telekabel*, since it involved blocking only a specific website and the affected users would presumably have an opportunity to learn of the problem when they could not access a website.[188] Users should therefore be all the more able to challenge a filtering mechanism that is not strictly targeted in the sense that it applies to all uploaded content.

Additional concerns arise from the fact that the effectiveness of the safeguards is entirely outsourced to profit-driven non-state actors for whom it is economically advantageous to overblock and avoid potential liability, rather than to ensure a fair balance with users fundamental rights. This leads up to a situation, where *"people's freedom of speech interests [are] hostage to the provider's economic considerations"*.[189]

---

[183] *Husovec,* Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p. 17; *Schwemer/Shovsbo,* What is Left of User Rights? Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime, Forthcoming in Paul Torremans (ed), Intellectual Property Law and Human Rights, 4th edition, 2020, p. 16. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3507542.

[184] *Senftleben,* Bermuda Triangle - Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market, p. 10. https://ssrn.com/abstract=3367219.

[185] Ibid. p. 9.

[186] Ibid.

[187] CJEU, C-314/12, ECLI:EU:C:2014:192 – *UPC Telekabel,* para. 57.

[188] *Keller,* Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling, GRUR Int 2020, p. 621.

[189] *Husovec,* Invisible Speech Harms of Delegated Enforcement: When is the EU Legislator Responsible? Forthcoming, p. 17.

7 Interference with Freedom to Conduct a Business

Article 16 CFR recognizes the right to conduct a business as a fundamental right. It is clear that licensing and filtering obligations impose costs and burdens on the OCSSPs and thereby interfere with their freedom to conduct a business. Since Article 17 CDSMD serves the aim of closing an alleged "value gap" that is based on the legislator's assumption that OCSSPs generate revenues from providing access to copyright protected material without duly compensating the rightsholders, it is clear that Article 17 CDSMD seeks to place a greater economic burden on the OCSSPs.

Whether Article 17 CDSMD amounts to a violation of the OCSSPs' freedom to conduct a business depends on whether the costs incurred by OCSSPs in order to comply with Article 17 CDSMD reflect a fair balance between their freedom to conduct a business and the right to intellectual property of rightsholders. In *Netlog*, the CJEU found that the contested filtering system failed to strike this balance and therefore violated Netlog's right to conduct its business. To reach that conclusion, the Court took into consideration what the contested injunction would require Netlog to do: to install a filtering system at its own cost that monitors most of the information stored by the host provider with no limitation in time.[190] According to the CJEU, such an injunction:

> *" […] would result in a **serious infringement of the freedom of the hosting service provider to conduct its business** since it would require that hosting service provider to install a **complicated, costly, permanent** computer system **at its own expense**, which would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48, which requires that measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly"* (accentuation by the authors).[191]

This assessment by the CJEU, which is based on the threefold burden of a system that is complicated, costly and permanent, may as well apply to the obligations placed on the OCSSPs by Article 17. As we have laid out above in chapters 2, 4 and 5, Article 17 CDMSD de facto requires, despite its technologically neutral wording, the implementation of automated filtering systems.

7.1 The Economic Impact of Article 17 on OCCSPs Can Be Immense

In its impact assessment, the Commission takes an utterly different stance than the CJEU in the *Netlog* decision, describing the impact of the Article 17 mechanism on the OCSSPs' freedom to conduct a business as follows:

> *"the **level of this impact is expected to be limited** due to the fact that the obligation is imposed on **services giving access to large amounts of protected content only**, that the option builds on existing voluntary practices and that technologies are increasingly available in the market which makes the implementation of the technology obligation easier for the services. This impact is further limited by the fact that the proportionality in the choice and in the deployment of effective content identification technologies will*

[190] CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog*, paras. 45 f.
[191] Ibid. para. 46.

allow to take into account the size and the nature of the individual services." (accentuation by the authors).[192]

This passage suggests that the Commission only intended to target large companies with the obligation to install costly filtering systems, which could either afford the expense or already relied on automated filtering technologies on a voluntary basis, and that a proportionality requirement would mitigate the effects on smaller businesses. Looking at the final version of the CDSMD, these assumptions do not seem to hold true.

Concerning the scope of application of Article 17 CDSMD, it is likely that not only large platforms like YouTube will meet the criteria laid down in Art 2 (6) CDSMD, but also smaller, less economically successful platforms and even platforms that only rarely encounter copyright infringements on their services. What is particularly striking is that the legal definition in Art 2 (6) CDSMD departs significantly from the corresponding Recital 62. While Recital 62 explains that the definition of OCSSP should target only online services, "that play an important role on the online content market by competing with other online content services, such as online audio and video streaming services, for the same audiences", the definition of OCSSPs in Art 2 (6) CDSMD contains no such qualifications.

A verbatim transposition of the definition of OCSSPs would cause the scope of application to drastically exceed the aim of the Directive as described in Recital 62. Because the legal definition in Art 2 (6) CDSMD does not reflect the criteria of Recital 62, but instead relies on the criterion "large amount of copyright-protected works", numerous service providers will potentially have to comply with the Art 17 liability mechanism, even if copyright infringements on these platforms are of no significance at all. Almost every service that hosts user-generated content hosts "large amounts" of works or other protected subject-matter, because almost any content can be protected by copyright or related rights (all photographs, short texts, audio snippets etc). Even news aggregators like reddit, which mostly host text in the form of user comments but nevertheless organise and promote the shared links to news stories for profit, or dating platforms like Tinder, which host photographs that for the most part have been created by the users themselves (selfies), would potentially have to implement the filtering technologies required by Art 17 (4) CDSMD, not to mention being forced to accept fairly priced licensing offers from rightsholders whose portfolios are irrelevant to their business models. In its impact assessment, the Commission did clearly not take this situation into account and false equated the presence of large amounts of protected materials with large numbers of infringements.

Art 17 (6) CDSMD limits the obligations of Art 17 (4) CDSMD to notice-and-takedown for "new OCSSPs" that have been available to the public in the Union for less than three years and which have an annual turnover below EUR 10 million, unless the number of unique monthly visitors to their services exceeds 5 million. This restriction is likely to have very limited practical relevance, since the criteria have to be met cumulatively so that even platforms that generate significantly less revenue than EUR 10 million will have to comply with Art 17 (4) CDSMD if they have been available for more than three years. This exception could even prove to be harmful to smaller service providers, if Member States conclude that OCSSPs that fail to meet

[192] Commission Staff Working Document, Impact Assessment on the modernisation of EU copyright rules, SWD(2016) 301 final, section 5.2.3.

the strict criteria of Article 17 (6) CDSMD must conversely be held to stricter standards than notice-and-takedown, regardless of the principle of proportionality.[193]

7.2 Proportionality Provision in Article 17 (5) CDSMD Falls Short

The central provision to mitigate the impact of Article 17 CDSMD on the OCSSPs' freedom to conduct a business is the proportionality principle laid down in Article 17 (5) CDSMD. When determining what OCSSPs have to do to comply with the best efforts obligations under Article 17 (4) CDSMD, a non-exhaustive list of criteria laid down in Article 17 (5) CDSMD, including the "the type, the audience and the size of the service and the type of works or other subject matter uploaded by the users of the service" as well as "the availability of suitable and effective means and their cost"[194] have to be taken into account.

While the principle of proportionality is an important means to strike a fair balance between competing rights, the proportionality clause in Article 17 (5) CDMSD falls short of this goal. The requirement of a case-by-case assessment based on the criteria of Article 17 (5) CDSMD comes at the cost of legal certainty for service providers that cannot determine, at the outset, what the law requires of them. Therefore, it will ultimately be for the courts to decide which obligations apply to which service providers. In the meantime, smaller service providers that decide to implement less costly and technically sophisticated solutions face the risk of direct liability for not having met the "best efforts" prescribed by Article 17 (4) CDSMD.

Another issue arising from the wording of Article 17 (5) CDMSD is that the requirement to consider "the type of works or other subject matter uploaded by the users of the service" is insufficient for platforms to conclude that the "best effort" obligation under Article 17 (4) CDSMD is limited to a single category of protected works. Therefore, OCSSP could be required to apply "best efforts" to block all kind of copyright protected content, regardless of the platform's target group and the prevalence of the content on the platform. OCSSPs could therefore be obliged to implement different filtering technologies pertaining to different kinds of contents, which would significantly increase the costs.[195]

The Commission's draft guidance on the implementation of Art 17 CDSMD underlines the understanding that Article 17 (4) and (5) CDMSD oblige OCSSPs to make best efforts to filter, and indeed license, all kinds of content that can theoretically be uploaded to their platform. In its guidance, the Commission states that OCSSP should:

> *"as a rule enter into negotiations with those rightholders that wish to offer an authorisation for their content,* ***irrespective of whether their type of content (eg. music, audio-visual content, images, text, etc...) is prevalent or is less common*** *on the website of the service provider. Nevertheless, pursuant to the principle of*

[193] The German Ministry of Justice has proposed a legal presumption that the imposition of filtering obligations on platforms with an annual turnover below EUR 1 million would be disproportionate. This proposal is reportedly being challenged by the State Minister for Culture, arguing that such presumption would violate Article 17 (6) CDSMD. Cf. *Krempl Urheberrechtsreform:* Altmaier macht gegen Nutzung von Inhalte-Schnipseln mobil. Heise online. https://perma.cc/PVP5-NKFB.

[194] Art 17 (5) CDSMD.

[195] Cf. *Engstrom/Feamster,* The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools, Engine, p. 14. https://www.engine.is/the-limits-of-filtering.

proportionality, in certain cases (notably in case of smaller service providers) a lower level of effort to obtain an authorisation may be expected for types of content which are less common on the website of a given service provider (e.g. for images or texts on a video-sharing platform).” (accentuation by the authors).[196]

If this interpretation regarding the best efforts to obtain an authorisation under Article 17 (4) (a) prevails, it is likely that the same applies for the obligations under Article 17 (4) (b) and (c). Since one category of work can easily be implemented in another (a work of literature, read aloud, can be included in an audio file, computer code can be included in a text file, a picture can be embedded in a video), OCSSPs have no means of categorically limiting user uploads to one category of works in order to keep their obligations under Article 17 (4) more manageable. The question of the applicability of the best efforts obligations to different categories of works is ultimately left to the courts, leaving the affected platforms in even greater legal and economic uncertainty.

Not only small platforms will be significantly affected in their freedom to conduct a business. A common argument for the proportionality of Article 17 CDSMD is that many of the platforms the legislator intended to target already use filtering technologies on a voluntary basis. Firstly, the costs for filtering technologies may significantly increase, because platforms may have to implement additional filtering systems for other categories of content.

Secondly, the filtering obligations deriving from Article 17 CDSMD can significantly deviate from the practice on platforms and further increase the platforms’ costs and aggravate the impact on other fundamental rights. For example, OCSSPs could be required to filter and identify even the shortest copyright-protected works, given that very short sound samples fall under the protection of copyright.[197] Simple content recognition technologies such as hash matching cannot detect extracts of works at all. More sophisticated technologies based on fingerprinting are able to detect partial matches, because they are based on an analysis of the contents of the work (such as the melody), rather than technical properties of the data file.[198] Consequently, the accuracy of fingerprinting is inversely correlated with the length of the match it is required to detect. The shorter the work that is claimed by a rightsholder, the less reliably can a filter match this work against large repertoires of similar copyright-protected material. The precision of existing filtering technologies would significantly suffer, should OCSSP be required to filter much shorter extracts of protected works than they currently detect on a voluntary basis, leading not only to higher costs for OCSSPs but also to much higher rates of false positives and collateral overblocking.

Thirdly, platforms like YouTube have limited the access to their filtering tools to certain rightsholders that fulfil a number of conditions and have, in the case of YouTube, to conclude a separate agreement to be able use YouTubes “Content ID” filter.[199] The fairness of these requirements that are currently unilaterally imposed by platform operators on rightsholders can of course rightfully be called into question. In fact, the very legality of these voluntary filtering efforts under Article 22 GDPR is questionable, insofar as they create significantly

[196] European Commission. 2020. Targeted consultation addressed to the participants to the stakeholder dialogue on Article 17 of the Directive on Copyright in the Digital Single Market, p. 6.
[197] CJEU, C-476/17, ECLI:EU:C:2019:624 – *Pelham,* para. 29.
[198] Cf. *Engstrom/Feamster,* The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools, Engine, p. 14. https://www.engine.is/the-limits-of-filtering.
[199] https://support.google.com/youtube/answer/1311402?hl=en.

detrimental effects on data subjects solely on the basis of automated decision-making.[200] The concerns expressed here are therefore not to be misunderstood as an endorsement of voluntary filtering mechanisms. The existing access restrictions to those filtering tools are merely mentioned here in order to illustrate the misguidedness of the European Commission's assumption expressed in its impact assessment[201] that the costs of existing voluntary filtering systems are comparable to those of potential future filtering obligations under Article 17 (4) CDSMD. This expectation is also unrealistic because the voluntary use of such technologies thus far has not given rise to liability in cases where these tools should fail to meet "high standards of professional diligence".[202]

Under Article 17 (4) CDSMD, platforms will have to give access to their systems to all rightsholders, since Article 17 CDSMD does not make a distinction between categories of rightsholders and a legal discrimination between larger and smaller rightsholders would in any case be difficult to justify. Once a rightsholder provides relevant and necessary information, the OCSSP will be bound by the obligations under Article 17 (4) CDSMD. Drastically increasing the number of rightsholders who use a filtering system can in turn lead to a multiplication of the expenses for operating the filtering system.

Third-party providers of filtering software are likely to drastically increase the price of their offerings not only due to increased demand, but also to account for the need to constantly update their reference databases to include reference files provided by a potentially boundless circle of rightsholders. The addition of large numbers of rightsholders to existing voluntary filtering mechanisms would also increase the incidence of overblocking caused by an increase in the total number of false claims.[203] Handling complaints about those false claims would in turn put significant economic burden on the platforms. Advocate General Saugmandsgaard Øe highlights in his opinion on the *YouTube* and *Cyando* cases that determining the validity of a rightsholder's claim can be a complex task, stating that: "It is clear from the order for reference in Case C-682/18 that a significant part of the judgment on appeal is dedicated to ascertaining whether, and to what extent, Mr Peterson holds the rights to the works concerned".[204]

7.3 What Are the Costs?

Considering the fact that the Commission did not take any of the considerations mentioned above into account in its impact assessment, it is very likely that the burden of costs and the

[200] *Electronic Frontier Foundation* Copyright Filters Are On a Collision Course With EU Data Privacy Rules. https://www.eff.org/deeplinks/2020/02/upload-filters-are-odds-gdpr.

[201] Commission Staff Working Document, Impact Assessment on the modernisation of EU copyright rules, SWD(2016) 301 final, p. 152. The same flawed assumption is expressed in the German Justice Ministry's impact assessment of its draft implementation law. Cf. *Bundesministerium für Justiz und Verbraucherschutz* Referentenentwurf für das Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes, p. 65.

[202] Article 17 (4)(b) CDSMD.

[203] A study on the notice-and-takedown system under the US Digital Millennium Copyright Act, which is in principle open to all rightsholders, has found that over 4 percent of takedown requests were fundamentally flawed, because they targeted content for which the notice sender clearly did not hold the rights. Cf. *Urban et al.*, Notice and Takedown in Everyday Practice. UC Berkeley Public Law Research Paper No. 2755628, p. 88. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628.

[204] CJEU, Joined Cases C-682/18 and C-683/18, ECLI:EU:C:2020:586 – *YouTube and Cyando* Opinion of Advocate General Saugmandsgaard Øe, fn. 182.

resulting interference with the OCSSPs' freedom to conduct a business will be more severe than the Commission expected.

In addition to the "purchase" of a filtering system, there are numerous other costs resulting from the implementation of Art 17 CDSMD. Operating a filtering systems involve human and technical resources. This includes development costs for the technical integration of external filtering products in the platform, as well as customer support for both rightsholders and users. OCSSPs will be required to verify information submitted by rightsholders that continuously submit new information and will have to provide that service for anyone who claims to be a rightsholder. Additional costs arise for the processing of users' appeals against mistaken or abusive automated claims. The operating costs as well as the number of false claims can be expected to significantly increase under Article 17 CDSMD as the filtering technology will have to be made available to a much larger number of rightsholders and the filtering of very short works such as audio samples can be required. The costs for the in-platform complaint and redress mechanism required by Article 17 (9) CDSMD are allocated entirely to the platforms. For larger and established service providers this constitutes a significant impact because of the increase in costs, but for smaller platforms that are potentially not even operating profitably and could rely on notice-and-takedown in the past, these costs are completely new and can amount to choking effects.[205]

Further costs as well as legal uncertainty arise from the cross-border nature of the services that OCSSPs provide. Under the *lex loci protectionis* principle generally prevailing in copyright law disputes[206], OCSSPs will have to use geo-blocking in order to comply with their potentially conflicting national obligations under Article 17 (4) and (7) CDSMD: OCSSPs have to prevent the upload of content that is illegal under one jurisdiction to avoid liability under Article 17 (4) CDSMD and keep it online in those jurisdictions where the content is legal in order to comply with their obligation in Article 17 (7) CDSMD. This already complex legal and factual situation for the OCSSPs could be somewhat mitigated if the Commission is correct in its assessment in its draft guidance that the complaint and redress mechanism in Article 17 (9) CDSMD should be implemented in line with the "country of origin" principle.[207] Should, however consumers be involved, the country of origin principle from Article 3 ECD is not applicable, because Article 3 (3) ECD and annex excludes contractual obligations concerning consumer contracts from the scope of application of Article 3 ECD. This puts another burden on the OCSSPs, that may have to implement complaint and redress mechanisms that comply with all national implementations. The level of protection for the consumers can substantially differ between the Member States, since Article 17 (7) CDSMD leaves the means to ensure that no legal content is blocked entirely to the Member States.

This already substantial economic burden will be complemented by licensing costs. Taking into account the draft guidance of the Commission that would require OCSSPs to enter into negotiations with rightsholders, irrespective of the type of content that is prevalent on the platform, these costs could become incalculable. Platforms would have to conclude license agreements for content that they have no interest in. The costs for licensing are hard to

[205] *Bridy,* The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform, Vanderbilt Journal of Entertainment & Technology Law, volume 22 (2020), p. 350.
[206] Art 5 (2) Berne Convention.
[207] European Commission. 2020. Targeted consultation addressed to the participants to the stakeholder dialogue on Article 17 of the Directive on Copyright in the Digital Single Market, p. 17.

predict, not least because of these legal uncertainties regarding the scope of the obligation to make best efforts to obtain licenses. However, in view of the fact that smaller platforms generate only little or no profit at all, they may lead to serious threat to their business models.[208]

7.4 Economic Impact and Balancing of Fundamental Rights

From what we have shown above, it is clear that the impact of Art 17 CDSMD on the OCSSPs' freedom to conduct a business is significant, since it may lead to a substantial economic burden, for larger and smaller platforms alike. Though the former may still be able to bear the costs, the latter may be threatened in their existence. Thus the question arises, if the impact of Article 17 CDSMD on the freedom to conduct a business corresponds to the effects in the cases *Netlog* and *Scarlet*, where the CJEU held that the implementation of the contested filtering systems would not strike a fair balance with the rightsholders' right to intellectual property enshrined in Article 17 (2) CFR.[209]

The main difference between the filtering system required by the statutory provisions of Article 17 CDSMD and the filtering systems required by the injunctions in *Netlog* and *Scarlet* is that the injunctions were limited to the application of filtering technologies that detect music, whereas Article 17 (4) CDSMD would potentially require OCSSPs to employ filtering technologies for the detection of multiple categories of works. The dispute in the main proceedings in *Scarlet* actually concerned an injunction requiring Scarlet to implement the third-party music filtering software Audible Magic,[210] which has been hailed by the European Commission as a comparatively cheap solution with limited functionality.[211] Still, the Court found the cost of this filtering technology to be disproportionate.

While Article 17 CDSMD contains safeguards for the OCSSPs, namely the proportionality principle in Art 17 (5) and the exception for new service providers in Art 17 (6) CDSMD, both safeguards are not suitable to achieve their goals and significantly mitigate the impact on the OCSSPs' freedom to conduct a business. In any case, Netlog would not have qualified as a new OCSSP within the meaning of Article 17 (6) CDSMD.[212] In addition, the costs for the implementation and the maintenance of a filtering system, based on the consideration outlined above, appear to be significantly underestimated by the Commission. This concerns both the costs for human and technical maintenance of a filtering system as well as the costs for licensing a third-party software.

---

[208] The German Ministry of Justice, in its economic impact assessment of its implementation proposal has calculated that an OCSSP with an annual turnover between EUR 1 and 2 million that would not benefit from the startup regime under Article 17 (6) CDSMD would have to expect compliance costs of at least EUR 175,000 annually, excluding the costs of licenses. These running costs would drive an OCSSP with a profit margin below 10 percent out of business. Cf. *Bundesministerium für Justiz und Verbraucherschutz* Referentenentwurf für das Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes, pp. 63 ff.

[209] CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog*, para 45; CJEU, C-70/10, ECLI:EU:C:2011:771 – *Scarlet*, para. 49.

[210] Le cour d'appel de Bruxelles, 9ème chambre, 28.1.2010, R.G.: 2007/AR/2424.

[211] Commission Staff Working Document, Impact Assessment on the modernisation of EU copyright rules, SWD(2016) 301 final, section 5.2.3.

[212] At the time, Netlog was being "used by tens of millions of inviduals on a daily basis", CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog*, para. 17.

Therefore, the impact of Article 17 CDSMD on the OCSSPs' freedom to conduct a business does not justify a different interpretation than in the cases *Netlog* and *Scarlet*. Insofar as, despite the safeguards, platforms will have to implement a complicated, costly and permanent technical solution at their own expense, Article 17 CDSMD fails to strike a fair balance between the OCSSPs' right to conduct a business and the rightsholders' right to intellectual property, thus violating Article 16 CFR.

8 Interference with Right to Data Protection

The liability mechanism introduced by Article 17 CDSMD is very likely to have a significant impact on the users' fundamental right to the protection of personal date enshrined in Article 8 CFR. As we have explained in chapters 2 and 5.1., Article 17 (4)(b) and (c) CDSMD lead to a de facto obligation to implement automated filtering systems. As described above, in order to be able to block content that matches information provided by rightsholders and prevent to prevent content from being uploaded (staydown), Article 17 (4) (b) and (c) CDSMD requires OCSSPs to implement automated filtering systems that screen every piece of user-uploaded content and match it against the information provided by the rightsholder. In chapter 4 we confirmed that this far-reaching filtering obligation is incompatible with the ban on general monitoring obligations under Article 15 (1) ECD and Article 17 (8) CDSMD. As the CJEU established in *Scarlet* and *Netlog*,[213] a filtering mandate constitutes an interference not only with the freedom of expression and information of users and the freedom to conduct a business of intermediaries, it also requires the mass processing of data related to the user uploads, which includes personal data.

8.1 Article 17 Requires Mass Processing of Personal Data

There is difficulty in identifying the personal data at issue, due to the abstract nature of the Directive and the technologically neutral wording of Article 17 (4) CDSMD. However, the implementation of filtering systems that meet the requirements of Article 17 (4) CDMSD require the algorithmic screening and matching of all uploaded content and will inevitably lead to the processing of personal data. The same applies to cases where the provider has to obtain a license that is intended to benefit the user.[214]

In order to upload content to the servers of an OCSSP, users will most likely need an account which contains personal data. The uploaded content usually remains connected to that account. Practically any content that is screened by the filtering system therefore contains personal data of the users. Even if users do provide personal data for the registration of an account, the processing of data to match an upload against the rightsholder's information requires the processing of metadata, including the IP-address of the uploader.[215] In *Breyer v Germany*, the CJEU has ruled that dynamic IP addresses constitute personal data if the IP address can lead to the identification of the data subject, even if it requires a combination

[213] CJEU, C-70/10, ECLI:EU:C:2011:771 – *Scarlet*, CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog.*
[214] Spindler, Gutachten zur Urheberrechtsrichtlinie (DSM-RL): Europarechtliche Vereinbarkeit (Artikel 17), Vorschläge zur nationalen Umsetzung und zur Stärkung der Urheberinnen und Urheber, p. 21.
[215] *Electronic Frontier Foundation* Copyright Filters Are On a Collision Course With EU Data Privacy Rules. https://www.eff.org/deeplinks/2020/02/upload-filters-are-odds-gdpr.

with other data to do so.[216] The Working Party on the Protection of Individuals with regard to the Processing of Personal Data (WP29) also considers that, without a shadow of a doubt, IP addresses constitute personal data.[217]

In the context of copyright-related filtering systems, the CJEU has confirmed that an injunction which requires the implementation of a filtering system affects the users right to data protection. The CJEU has addressed the interferences of permanent filtering mandates with the users' right to data protection in the cases *Netlog* and *Scarlet*. In that context the CJEU confirmed that IP addresses constitute personal data because the IP addresses facilitate the identification of users that upload unlawful content.[218] In the case of the host provider Netlog, the Court further confirmed that the contested filtering system would involve the processing of personal information insofar as data in connection with the profiles that users created on the platform is involved.[219] In both cases the Court found that the contested injunctions would not strike a fair balance between the right to intellectual property on the one hand and, inter alia, the right to protection of personal data on the other.[220]

As regards the processing of personal data, the filtering mechanism prescribed by Article 17 CDSMD is analogous to the mechanisms required by the injunctions in *Netlog* and *Scarlet*. The Court held that the contested injunctions required the monitoring of large parts of the information stored by the provider and that the filtering involved the processing of personal data because of a connection of the processed data with user profiles on a platform (*Netlog*) or the processing of the users' IP addresses (*Scarlet*).[221] Therefore, the interference with the users' right to data protection induced by Article 17 CDSMD is comparable to those in the cases *Netlog* and *Scarlet*. One cannot deduce from these decisions to what extent the CJEU based the rejection of the filtering systems on the interference in Article 8 CFR, but the fact that the CJEU explicitly based the rulings on these considerations shows that the Court places a substantial weight on the interference with Article 8 CFR.

What distinguishes the Article 17 mechanism from the contested injunctions in *Netlog* and *Scarlet* is the fact that Article 17 CDSMD includes a specific provision aimed at safeguarding the right to data protection. Article 17 (9) CDMSD states that the directive shall "not lead to any identification of individual users nor to the processing of personal data, except in accordance with Directive 2002/58/EC and Regulation (EU) 2016/679". But, as with the safeguards for the freedom of expression and information, this obligation of result is not sufficient to safeguard the users' right to data protection, because it lacks enforceability, mandatory transparency and state oversight.

8.2 Automated Decision-Making Aggravates Interference with Fundamental Rights

[216] CJEU, C-582/14, ECLI:EU:C:2016:779 – *Breyer v Germany.*
[217] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data. 01248/07/EN WP 136.
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.
[218] CJEU, C-70/10, ECLI:EU:C:2011:771 – *Scarlet*, para. 51.
[219] CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog*, para. 49.
[220] CJEU, C-70/10, ECLI:EU:C:2011:771 – *Scarlet*, para. 53; CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog*, para. 51.
[221] CJEU, C-70/10, ECLI:EU:C:2011:771 – *Scarlet*, para. 53; CJEU, C-360/10, ECLI:EU:C:2012:85 – *Netlog*, paras. 45, 49.

The implementation of Article 17 CDSMD may lead to fully automated decision-making, which has prompted commentators to raise serious data protection concerns.[222] Secondary EU law addresses the risks that arise from automated decision-making through Article 22 GDPR, which grants data subjects special protection from those risks. Article 22 GDPR is rooted in EU primary law, namely Article 8 CFR. Article 22 GDPR shows that the EU legislator considers automated decision-making to pose a particularly high risk to the data subject. Automated decision-making constitutes an especially severe interference with Article 8 CFR, because it would leave the data subjects at the mercy of a purely technical and untransparent process, without being able to comprehend the underlying assumptions and evaluation criteria and, if necessary, to assert one's right before an independent judicial body.[223] While Article 17 (9) CDSMD requires that users of OCSSPs have access to a court or relevant judicial authority, it fails to confer the necessary information rights on users that would allow them to effectively challenge fully automated decisions that negatively affect them.

Against this background, the impact of Article 17 CDMSD on the users' right to data protection is evident. As we have discussed above in chapter 5, the introduction of the Article 17 liability mechanism will lead to the preventive blocking and removal of potentially lawful content, solely based on the decision of an automated filtering system. This mechanism leads to prior restraint of the users' right to freedom of expression and information whereas specific safeguards, including human review[224] and judicial redress, apply only ex-post. Article 17 (4) CDSMD therefore leaves the users in a very vulnerable position. Their right to data protection is not sufficiently safeguarded when they are made subject to an automated decision that is relevant to exercise their freedom of expression. Automated decision-making in the context of Article 17 therefore has a considerable impact on fundamental rights. Given the importance of communication on the internet for the freedom of expression, this interference can only be justified in exceptional circumstances.

The risks of automated data processing are also addressed by the CJEU in its opinion on the PNR Agreement between the EU and Canada.[225] The Court holds that automated analyses of Passenger Name Records (PNR) involves some margin of error and that positive results obtained from the automated processing must therefore be subject to an individual re-examination by a human.[226] In the light of the impact that automated data processing in the context of the Article 17 mechanism has on the users' fundamental right to freedom of expression and information, the decision to block or remove potentially lawful content should not be solely based on an automated decision either.

Article 8 CFR is not guaranteed absolutely, it is subject to the general reservation of Article 52 (1) CFR. However, in order to legitimately restrict interferences with Article 8 CFR, it is

---

[222] Cf. Electronic Frontier Foundation, Copyright Filters Are On a Collision Course With EU Data Privacy Rules; *Stalla-Bourdillon* Data Protection and Copyright: Could Art. 29 WP guidance on automated decision-making "help" with filters? https://perma.cc/85EP-NH6W.

[223] *Von Lewinski*, in: BeckOK Datenschutzrecht, Wolff/Brink, 33. Edition, Art 22 DSGVO, para. 2.

[224] The requirement in Article 17 (9) CDSMD that "decisions to disable access to or remove uploaded content shall be subject to human review" could be interpreted to apply to all blocking decisions, but the placement of this statement in a sentence about the complaint and redress mechanism suggests that human review is only mandatory after a complaint about a (fully automated) blocking decision has been made.

[225] CJEU (Grand Chamber), Opinion 1/15 of the Court, EU – Canada Passenger Name Record (PNR) Agreement, ECLI:EU:C:2017:592.

[226] Ibid. Para. 173.

necessary that Article 17 CDSMD is compliant with the principle of proportionality when balanced against other fundamental rights.[227] In any case, the liability mechanism must not lead to an obligatory systematic analysis and processing of information relating to the user profiles created within the service.[228]

9 Conclusion

Even considering the rather narrow scope of Poland's action for annulment of Article 17 (4)(b) CDSMD and parts of Article 17 (4)(c) CDSMD *in fine*, our analysis shows that the action has merit. Although the specific provisions of Article 17 CDSMD do not explicitly oblige service providers to employ automated ex-ante filtering of all user uploads, service providers are left with no other choice than to employ them in order to limit their liability for copyright infringements of their users. As we have shown, these provisions therefore constitute a general monitoring obligation, which is incompatible with the Charter. According to the case law of the CJEU, an obligation to monitor all user uploads for specific protected works constitutes a general monitoring obligation, unless it is limited to specific uses of those works that a court has identified as infringing, thus eliminating the risk of overblocking.

In our overall assessment, the provisions in dispute are not capable of achieving a fair balance between the fundamental rights concerned. Art. 17 CDSMD primarily serves to protect the intellectual property of rightsholders, even at the cost of the artistic expression of others.[229] The result of the liability mechanism imposed on platforms is that the protected interests of the rightsholders are asserted in a way that does not take sufficient account of the fundamental rights of the other stakeholders, most notably the freedom of expression and information of users and their right to protection of personal data, as well as the freedom to conduct a business of platform operators.

The liability mechanism of Article 17 (4) CDSMD constitutes a particularly serious interference with the freedom of expression, because it constitutes a form of prior restraint. User uploads are blocked before a judicial decision on the lawfulness of the information can be made. Measures that result in overblocking of permissible acts of communication have consistently been rejected by the courts as incompatible with the right to freedom of expression and information.

In cases in which it is uncertain whether a use of content is legal or not, it is not reasonable to have the freedom of expression recede behind the economic interests of the rightsholders. Rightholders must rather accept to temporarily tolerate an illegal use. Such a use can still be compensated subsequently. In contrast, due to the fast pace of online communication, a comparable redress in favour of users whose legal expressions were blocked is not conceivable.

Our analysis shows that the EU legislator has failed to meet its obligation to define the scope of the limitation of fundamental rights in Article 17 CDSMD. The view that Article 17 CDSMD

[227] *Specht-Riemenschneider*, Leitlinien zur Umsetzung des Art. 17 DSM-RL aus Verbrauchersicht, p. 45 with specific considerations.
[228] *Specht-Riemenschneider*, p. 45 with reference to CJEU, *Scarlet*, para. 51.
[229] Advocate General Saugmandsgaard Øe, Opinion, Joined Cases C-682/18 and C-683/18, ECLI:EU:C:2020:586 – *YouTube* and *Cyando*, para. 243.

could be implemented in a manner that will avoid all overblocking of legal uses[230] is ultimately unconvincing and contradicted by all available evidence about Member States' implementation efforts to date. To the extent that the EU legislator has introduced safeguards in the provisions of Article 17 CDSMD, those safeguards lack enforcement provisions and are insufficiently precise to ensure that the users' rights to freedom of expression and information are guaranteed.

The legislator has based its assessment of the impact of Article 17 CDSMD on the freedom to conduct a business on questionable assumptions that overestimate the capabilities of content recognition technologies and underestimate their costs. Finally, Article 17 CDSMD subjects users to fully automated decisions that interfere with their fundamental right to data protection.

The deadline for implementation of the CDSMD into national law is likely to lapse before the CJEU will be able to deliver its judgement in *Poland v European Parliament and Council*.[231] Given the serious fundamental rights implications of Article 17 CDSMD identified in this study, Member States are placed in a dilemma – having to choose whether to implement a provision that may soon be declared incompatible with the Charter by the Court, or risk infringement proceedings by the European Commission for failing to meet the transposition deadline.

The European legislator would be well-advised to put greater emphasis on the fundamental rights impact of new legal frameworks for online content moderation at the outset. In this context, the very critical stance that the European Parliament has adopted towards filtering technologies[232] in the ongoing negotiations on the proposed Terrorism Regulation, as well as regarding the future proposal for a Digital Services Act, is to be welcomed. While the outcome of *Poland v European Parliament and Council* is uncertain, it is clear that many of the issues with Article 17 CDSMD could have been avoided if the legislator had more carefully considered the provision's consequences for all affected parties.

[230] Specht-Riemenschneider, Leitlinien zur nationalen Umsetzung des Art. 17 DSM-RL aus Verbrauchersicht, pp. 48, argues that technical user protection could establish a fundamental rights-compliant situation. This would require the widest possible differentiation between legal and illegal content by the OCSSPs and sufficient user rights. In fact, these requirements mitigate the adverse effects to the detriment of the users. Nevertheless, the view is ultimately not convincing, as it does not address the problem described fundamentally.
[231] Member States are required to implement the CDSMD by 07.06.2021. The opinion of Advocate General Saugmandsgaard Øe in *Poland v European Parliament and Council* is expected on 22.04.2021.
[232] See chapter 1 above.