

Mandatory Filtering Does Not Always Violate Freedom of Expression: Important Lessons from Poland v Council and European Parliament (C-401/19)

Martin Husovec, LSE Law

Can legislatures task machines with deciding when people can speak online? And what safeguards must be put in place by the Union and national legislatures to make us safe from potential abuses? These are the core questions at the heart of a complex copyright case concerning the validity of a provision in an EU Directive. The copyright complexity of the *Republic of Poland v European Parliament and Council of the European Union*, Case C-401/19 hides many valuable lessons for the protection of fundamental rights, digital policy, and copyright law in the European Union. This case note will try to unpack the most important ones: (a) the central responsibility of the EU legislature for the quality of its legislation, (b) the developing body of case law of the Court concerning automated decision-making, and (c) consequences for the national implementation of Article 17 of the Copyright DSM Directive after the judgment.

Introduction

To discuss the disputed provision without contextualising what preceded its adoption would be missing the forest for the trees. Article 17 of the Digital Single Market Copyright Directive¹ is an embodiment of a unique political struggle. Severine Dussolier aptly summarised it as a “monster provision”, referring to “its size and its hazardousness”.² The echoes of the controversies were heard even in Luxemburg. Advocate General reviewing the legislation noted that the legislative “process has also been marked by intensive lobbying campaigns on the part of the economic operators concerned and demonstrations of opposition from part of civil society, academic circles and advocates for freedom of expression”.³

How did it ever come to this?

Before the adoption of Article 17, providers of digital services, such as YouTube, did not have to license copyrighted content uploaded by users that they were not aware of. This followed from EU copyright law⁴ but was informed by the existence of liability exemptions introduced two decades ago to coordinate legislation in the (digital) internal market.⁵ The providers were mostly required to take down copyright-infringing content once they were notified. This imposed burden on rightsholders who had to detect and notify content. Although bigger providers, such as YouTube, would offer their own tools to detect infringements on their services, right holders were inevitably forced to choose between removal and no profit, or toleration of infringement in exchange for a share from advertising. Many right holders decided for the latter, however, feeling bitter resentment about the outcome.

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

² Séverine Dusollier, “The 2019 Directive on Copyright in the Digital Single Market: Some progress, a few bad choices, and an overall failed ambition” (2020) 57 Common Market Law Review 979–1030, 1008.

³ AG Opinion in Case C-401/19, *Poland*, para 23.

⁴ This was clarified in Joined Cases C-682/18 and C-683/18, *YouTube and Cyando*, ECLI:EU:C:2021:503.

⁵ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (2000) OJ L 178, p. 1–16.

Thus, the goal behind Article 17 was to solve a legitimate grievance of right holders – their low bargaining power vis-à-vis platforms that enabled the exploitation of their works.⁶ The music industry strongly lobbied around the world “to fix” the digital licensing of content on online sharing platforms.⁷ The most contested part was not the underlying problem of inadequate remuneration, but the proposed legislative solution to it. Once the proposal was met with heavy criticism and led to protests in the streets in the Member States,⁸ the political process turned into an unusual spectacle of European politics.⁹

The European Commission at first thought that it could achieve the change of law by only “clarifying” the law in the recitals of its 2016 proposal.¹⁰ This approach was broadly rejected. The legislative process in 2016-2019 saw several iterations of the original idea that content uploaded by users shall be licensed by platforms or filtered away.¹¹ The provision was written and re-written mostly for music licensing on video-sharing platforms. Eventually, the Union legislature settled on the solution that is now in Article 17 – a right that is directly owed by platforms to authors, performers, and other copyright investors.¹² Its goal is twofold: increase the amount of money raised through licensing and put the costs of enforcement mostly on providers. The latter goal, however, threatened to cause collateral damage to citizens whose speech will be removed by inadequate technology implemented to satisfy the legal mandate.

With the rough start, the provision did not enjoy much of a happy landing either. The end of the legislative process was only a stopover. The complexity of the provision immediately attracted wide disagreements about what the law says, and what it allows the Member States to do. Most of the Member States wanted to only copy and paste it, including those that originally opposed it, constantly worried to reopen the old wounds. Other countries, like Germany and Austria, preferred to adapt it, partly to appease their young electorate. Poland decided to use Article 17 as a political tool in its criticism of Brussels and sought its invalidation on the ground of freedom of expression. The European Commission came with very extensive guidance that probably overstepped its mandate.¹³

⁶ Séverine Dusollier, “The 2019 Directive on Copyright in the Digital Single Market: Some progress, a few bad choices, and an overall failed ambition” (2020) 57 *Common Market Law Review* 979–1030, 1008 ff.

⁷ For a scholarly view from the proponents, see Daniel L. Lawrence, *Addressing the Value Gap in the Age of Digital Music Streaming* (2021) 52 *Vanderbilt Law Review* 511-543.

⁸ Felix Reda, “EU copyright reform: Our fight was not in vain”, available at <<https://felixreda.eu/2019/04/not-in-vain/>> (analysing the magnitude of the protests and their impact).

⁹ The Commission’s website officially called the opposition “mob” which was allegedly created by Big Tech companies “to save the dragon and slay the knight” (<https://techmonitor.ai/technology/data/european-commission-mob>). The MEP responsible for shepherding the legislation through the European Parliament insisted that people protesting upload filters just do not understand the law. It was speculated the German government’s opposition to the proposal was traded for French government’s opposition to – of all things – a gas pipeline to Russia, Nordstream 2 (<https://www.forbes.com/sites/davekeating/2019/02/08/why-did-france-just-save-nord-stream-2/?sh=252ffa026055>). Finally, the UK and British MEPs that supported the legislation, eventually refused to implement it after exiting the EU.

¹⁰ Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market COM/2016/0593 final, see Recital 38 and Article 13.

¹¹ See for the mapping, Martin Husovec, “How Europe Wants to Redefine Global Online Copyright Enforcement” In: Tatiana Eleni Synodinou (ed.), *Pluralism or Universalism in International Copyright Law* (Kluwer law, 2019).

¹² Article 17 grants right to “the rightholders referred to in Article 3(1) and (2) of Directive 2001/29/EC”.

¹³ Communication from the Commission to the European Parliament and the Council Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final.

This small preview should be enough to make the point that while Article 17 is about a relatively narrow question of copyright policy, it triggered almost universal conflicts among the stakeholders, in academia and among the Member states. Based on my observation, to this date, most of the actors of the debates do not have good memories of it. This backdrop is crucial to understand the choice that the Court of Justice of the European Union faced. If it invalidated the provision, that would likely have been the end of the EU legislative debate for a long time – as no one seemed interested to start anew. But because the Court rather re-interpreted it, and put pressure on the Member States, it narrowed the impact, directed the attention to several important practical questions and avoided fragmentation within the EU.¹⁴ From the harmonisation standpoint, it was the best choice; from the fundamental rights perspective, the Court signalled problems which the EU legislature in the meantime stepped in to solve in another legislation.

Article 17 DSM Directive

Article 17 of the DSM Copyright Directive¹⁵ is a lengthy provision that could be summarised as follows: paragraphs (1) and (2) extend and modify the exclusive rights, together with Article 2(6); paragraph (3) exempts the new regime from the horizontal rules; paragraph (4) exempts some situations from the liability under paragraph (1); paragraph (5) and (6) qualify the obligations; paragraph (7) to (10) includes some basic sketch of safeguards. I quote below the most important parts:

Use of protected content by online content-sharing service providers

1. Member States shall provide that an online content-sharing service provider performs an act of communication to the public or an act of making available to the public for the purposes of this Directive when it gives the public access to copyright-protected works or other protected subject matter uploaded by its users. (...)
4. If no authorisation is granted, online content-sharing service providers shall be liable for unauthorised acts of communication to the public, including making available to the public, of copyright-protected works and other subject matter, unless the service providers demonstrate that they have: (a) made best efforts to obtain an authorisation, and (b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information; and in any event (c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b). (...)
7. The cooperation between online content-sharing service providers and rightholders shall not result in the prevention of the availability of works or other subject matter 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. (...)

Platforms that allow users to share content (e.g., YouTube) are subject to a special regime *if* their main purpose is to store and disseminate to the public large amounts of copyrighted material which they organise and promote for-profit (Article 2(6)). Unlike other platforms allowing storage, the “online content sharing service providers” (OCCSPs) must take a license from copyright holders. It means that an OCCSP should in theory clear rights and pay for every user-uploaded content (e.g., a video) that includes someone else’s works (e.g., music). In contrast, platforms that are outside this special regime are

¹⁴ However, the fallout of the invalidity ruling would have been much more complicated, as national implementation would already exist, and would not be always pre-empted by EU law.

¹⁵ Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (2019) OJ L 130.

exempted from liability for user uploads. Unless they contribute to the infringing actions of their users, they must in principle only act upon notifications they receive.

But since no platform can predict what will be uploaded on their service, OCSSPs must only try to make “best efforts to obtain an authorisation” from right holders (Article 17(4)(a)). Moreover, not every copyright holder might be interested to license their protected material to OCSSPs (e.g., movie studios). Right holders can thus deny granting such a license and request OCSSPs to engage in “best efforts to ensure the unavailability of specific” protected material (Article 17(4)(b)). Finally, only if right holders require no help with filtering and do not wish to license their material, OCSSPs can resort to simple handling of notifications.

The basic choreography of Article 17 thus can be described as a *license-first and filter-second regime*.

While filtering is not in the text of the provision, there are very limited ways how to “ensure the unavailability” or “to prevent future uploads” of protected material without resorting to content recognition tools which compare uploaded content with reference databases. Essentially, the only other way is acting upon meta-data of the past or suspected infringers, which is far from equally effective. As a result, the law de facto demands that automated tools, the filters, are relied upon to make decisions before such content is published online. The problem with this demand is that technologies available today are known to be *technically sophisticated but legally blind*.

Content recognition technologies can in real-time trace the borrowing of split-seconds of music among people across the globe, but they can say nothing about whether such borrowing is legally justified (e.g., for citation or parody). In other words, these tools are sophisticated detection mechanisms but very unsophisticated assessment tools. However, by configuring these tools to detect and block only some “matches” between suspected infringing content and the files in the references databases (e.g., borrowing over 50% of a song), the tools can make detections that are going to be also overwhelmingly legally accurate. The question of the use of filters is therefore about two separate issues: a) the technological maturity of machines entrusted to make decisions about blocking of user-general content and b) the sensitivity of their configuration.

Article 17 says nothing about concrete technologies that must be used by providers. However, it comes up with the following three legal requirements:

- the compliance cannot go beyond requiring “proportionate” efforts (Article 17(5)), which adjust to various types of content, size of providers, and technology’s availability and costs,
- the reliance on technologies “shall not result in the prevention of the availability” (Article 17(7)) of lawful material and in “no way affect legitimate uses” (Article 17(9)) of the protected material, the effect known as “over-blocking”, and
- the required efforts shall not amount to a “general monitoring obligation” (Article 17(8)).

Finally, the use of these technologies shall be made subject to the following set of procedural safeguards:

- any complaints of affected users who posted the content must be subject to an expedient and effective redress mechanism that involves humans (Article 17(9)),
- out-of-court redress mechanisms shall be available for the settlement of disputes (Article 17(9)),
- access to a judicial authority to assert the use of an exception or limitation shall be established in the national law (Article 17(9)) and

- stakeholder dialogues shall be organised by the European Commission to establish the best practices, which should involve sharing of “adequate” information with users’ organisations (Article 17(10)).

The Republic of Poland decided to challenge the constitutionality of Article 17 on three main grounds. Firstly, the provision, or its part, requires preventive filtering before the material goes online which, in its view, violates the essence¹⁶ of the right to freedom of expression enshrined in Article 11 of the EU Charter of Fundamental Rights.¹⁷ Preventive filtering as a measure is an aggravated interference because it is general, applies before the publication of the content, and is carried out automatically by algorithms. Such a setup is likely to lead to the blocking of lawful material. Secondly, there are alternative measures that the EU legislature could choose but did not.¹⁸ And finally, the EU legislature did not draft the law with sufficient precision and failed to introduce adequate safeguards to mitigate the risks of abuse.¹⁹

Consequently, Poland sought the annulment of Article 17(4)(b) and (c) to repeal the obligation to introduce upload filters or annulment of the entire provision. Despite the lack of enthusiasm for Article 17 among some Member States, no other state wanted to appear to support Poland in its legal action. On the contrary, Spain and France, along with the Parliament, Council and Commission provided opposition to Polish claims. They argued that the EU legislature itself does not limit freedom of expression and denied that the impact of the provision can be attributed to the EU legislature.²⁰ Alternatively, even if the EU legislature is responsible, the law preserves “the fair balance between the rights and interests involved” and in any case “comprises a comprehensive system of safeguards”.²¹

The Advocate General's Opinion

The Opinion in the case was delivered by Advocate General Henrik Saugmandsgaard Øe, a Danish jurist, who authored an extensive, rich, and very thoughtful analysis. AG was of the view that Article 17 should remain valid law and only needs to be re-interpreted in light of the fundamental rights at stake. The Court’s decision closely follows his analysis, with one minor but important difference: the standard of acceptable filtering technologies.

AG’s Opinion provides the best analysis of the problem of delegated enforcement among the highest European courts to date. Delegated enforcement describes a situation when the law expects platforms to act as enforcers of the law, by entrusting them with various tasks, such as the removal of content. Many states often try to disclaim any responsibility for how legislation is internalised by firms, arguing that those actions cannot be attributed to the lawmaker. AG cuts through these objections.

He positions the problem within the latest ECtHR case law²² and concludes that “[t]he legislature cannot delegate such a task and at the same time shift all liability to those providers for the resulting interferences

¹⁶ Art 52(1) CFR.

¹⁷ Case C-401/19, *Poland*, paras 40 ff. and 59 ff.

¹⁸ Case C-401/19, *Poland*, para 61.

¹⁹ Case C-401/19, *Poland*, para 59 ff.

²⁰ Case C-401/19, *Poland*, para 43.

²¹ Case C-401/19, *Poland*, para 62.

²² ECtHR, *Costello-Roberts v. the United Kingdom*, Appl. No. 13134/87, CE:ECHR:1993:0325JUD001313487, judgment of 25 March 1993, para 27 (‘the State cannot absolve itself from responsibility by delegating its obligations to private bodies or individuals’).

with the fundamental rights of users”.²³ In AG’s view, the state is responsible for the failings of firms which are legally expected to enforce the law, and so is the EU legislature in this case. As a result, legislatures must control the “beast” that they have created. In AG’s view, which is then endorsed by the Court,²⁴

“where the limitation of fundamental rights stems from the EU legislation itself, and is therefore attributable to the EU legislature, as is the case here, the EU legislature bears a significant share of the responsibility in that regard. It cannot, in such a case, leave to the Member States – or, a fortiori, the service providers responsible for implementing that legislation – the task of establishing such safeguards. On the contrary, it must define at the very least its substance.”

As discussed later, Advocate General next lays the groundwork for the Court’s approach. He proposes to look beyond the wording of Article 17 at its (likely) actual effects.²⁵ He also eloquently formulates a general heuristic to assess when the risks of over-blocking are present as follows:²⁶

“a risk of an ‘over-blocking’ exists, generally, where public authorities hold intermediary providers liable for illegal information provided by users of their services. In order to avoid any risk of liability, those intermediaries may tend to be overzealous and excessively block such information where there is the slightest doubt as to its lawfulness.”

The structure of his analysis is followed closely by the Court and therefore analysed below. In a nutshell, AG denies violation of the essence of the right and does not see disproportionality or insufficiency in safeguards in Article 17’s design. He argues that the requirement to avoid over-blocking in Article 17(7) acts as a counterforce to the tendency of overzealous enforcement because it obliges to the result.²⁷

AG proposed to narrow down the permissible filtering by linking it with the previous case law on injunctions. He proposed to rely on the concept of “manifestly illegal content”, which would include content which has been subject to judicial determination, or whose illegality can be established “without, inter alia, the need for contextualisation” and is thus obvious “from the outset”.²⁸ This standard was proposed by some academics and the European Commission as a way to limit the over-blocking effects.²⁹ The idea is similar to the Court’s final position, that is, filters should be configured according to what they can do.³⁰ It is driven by the Advocate General’s concern that the providers would have been otherwise

²³ AG Opinion in Case C-401/19, *Poland*, para 84.

²⁴ AG Opinion in Case C-401/19, *Republic of Poland v European Parliament, Council of the European Union*, ECLI:EU:C:2021:613, para 151.

²⁵ AG Opinion in Case C-401/19, *Poland*, para 86.

²⁶ AG Opinion in Case C-401/19, *Poland*, para 142.

²⁷ AG Opinion in Case C-401/19, *Poland*, para 165.

²⁸ AG Opinion in Case C-401/19, *Poland*, paras 197, 201-202.

²⁹Communication from the Commission to the European Parliament and the Council Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final (“automated blocking, i.e. preventing the upload by the use of technology, should in principle be limited to manifestly infringing uploads. (..) other uploads, which are not manifestly infringing, should in principle go online and may be subject to an ex post human review when rightholders oppose by sending a notice.”). See also João Pedro Quintais, Giancarlo Frosio, Stef van Gompel, Bernt P. Hugenholtz, Martin Husovec, Bernd Justin Jütte, and Martin Senftleben, “Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics”, 10 (2019) JIPITEC, 277-282.

³⁰ AG Opinion in Case C-401/19, *Poland*, para 211.

“turned into judges of online legality, who are responsible for coming to decisions on legally complex questions”.³¹

While AG presented a narrow reading of the filtering mandate,³² he considered that OCSSPs could be required to employ humans to manually review automatic matches.³³ Advocate General’s primary concern seems to have been how humans, augmented by machines, would be eventually able to make correct decisions in absence of initial notifications. The best efforts in Article 17(4), in his view, only concern content which is manifestly infringing.³⁴

The weakness of his argument was that what humans might consider obvious machines can still find complex. Thus, the pressure on follow-on human moderation could be immense. The Court seems to be much more conscious of this. The Court’s final standard is more technology-focused; however, its application is also broader because it applies to *any* re-uploads.

AG accepted the safeguards to be sufficient in their totality. However, he further considered that national implementations should be accompanied by transparency,³⁵ state supervision,³⁶ sanctions for violations of users’ rights,³⁷ and anti-abuse provisions.³⁸ Article 17 did not have to include such safeguards either because of the principle of procedural autonomy of the Member States³⁹ or because the area of application “concerns a technical field”.⁴⁰ As a result Article 17, if re-interpreted, should remain valid.

The Grand Chamber ruling

The ruling starts with assessing the admissibility of the claims. Similarly, as the Advocate General, the Court notes that annulment of only parts of Article 17 would have the effect of altering the substance, by creating a liability regime that would be “substantially different” and “more favourable to those providers”.⁴¹ In such situations, when the partial annulment would be objectively assessed, “alter the spirit and substance of the act”,⁴² the various components of the provision must be held *non-severable*. If an issue is „not severable from the remainder of (..) the principal head of claim, seeking annulment of those provisions only, is inadmissible”.⁴³ In the case at hand, this eventually was not a problem because Poland alternatively sought invalidation of the entire provision which can be severed from the rest of the Directive.⁴⁴ On this basis, the Court proceeds to evaluate the Polish challenge as relating to the entire provision.

Is the EU legislature responsible?

³¹ AG Opinion in Case C-401/19, *Poland*, para 197.

³² AG Opinion in Case C-401/19, *Poland*, para 203.

³³ AG Opinion in Case C-401/19, *Poland*, para 211 and footnote 245.

³⁴ AG Opinion in Case C-401/19, *Poland*, para 205.

³⁵ AG Opinion in Case C-401/19, *Poland*, para 212.

³⁶ AG Opinion in Case C-401/19, *Poland*, para 212 and footnote 249.

³⁷ AG Opinion in Case C-401/19, *Poland*, footnote 249.

³⁸ AG Opinion in Case C-401/19, *Poland*, footnote 251.

³⁹ AG Opinion in Case C-401/19, *Poland*, footnote 249.

⁴⁰ AG Opinion in Case C-401/19, *Poland*, para 151.

⁴¹ Case C-401/19, *Poland*, paras 17 and 20.

⁴² *Ibid.*

⁴³ Case C-401/19, *Poland*, para 21.

⁴⁴ Case C-401/19, *Poland*, para 22.

The Court first tackles the argument presented by the Council and Parliament that the EU legislature cannot be attributed how Article 17 is implemented in practice once it is implemented by the Member States.⁴⁵ As a result, the liability regime – best efforts licensing coupled with best efforts filtering upon request – which is at the heart of the provision cannot limit the right to freedom of expression and information of users. The judgment does not include specifics of this argument, but the rationale seems to be that the EU legislature cannot be held responsible for what the Member States and ultimately private parties will do during the implementation. The Court rejects the argument stating that “limitation [on the right to freedom of expression]⁴⁶ is attributable to the EU legislature since it is the direct consequence of the specific liability regime”.⁴⁷ By doing so, the Court fully follows the reasoning given by the Advocate General who concluded that “[t]he legislature cannot delegate” risky tasks to private parties “and at the same time shift all liability to those providers for the resulting interferences with the fundamental rights of users”.⁴⁸ The Court proceeds with an analysis of Article 17 as a form of state interference, focusing on *likely* real-world effects of the law on individuals. This framing again follows from the AG’s Opinion, which was firmly grounded in the ECtHR case law.⁴⁹

How important is user-generated content?

The Court is equally quick to highlight the internet’s special place among the technologies facilitating freedom of expression. Luxembourg judges not only reiterate equivalence between Article 10 ECHR and Article 11 CFR but also largely absorb Strasbourg’s latest case law.⁵⁰ Judges highlight that the internet has become “the principal means by which individuals exercise their right to freedom of expression and information”, which is facilitated by “accessibility”, and “capacity to store and communicate vast amounts of information”.⁵¹

The providers carrying user-generated content, such as OCSSPs, thus “play an important role in enhancing the public’s access to news and facilitating the dissemination of information in general, with user-generated expressive activity on the internet providing an unprecedented platform for the exercise of freedom of expression”.⁵² This is why even outside of this special regime, freedom of expression and information must be taken seriously.⁵³

The essence of the right to freedom of expression and information

With this starting point, the Court proceeds to analyse the scope of interference instigated by Article 17. Agreeing with Advocate General, judges note that “automatic recognition and filtering tools” resulting in “a prior review” are essentially the only ways to implement the provision’s mandate. The Court admits

⁴⁵ Case C-401/19, *Poland*, para 43.

⁴⁶ Case C-401/19, *Poland*, para 55.

⁴⁷ Case C-401/19, *Poland*, para 56.

⁴⁸ AG Opinion in Case C-401/19, *Poland*, para 84.

⁴⁹ AG Opinion in Case C-401/19, *Poland*, paras 82 and 83, footnote 91.

⁵⁰ Case C-401/19, *Poland*, para 46, citing ECtHR, *Cengiz and Others v. Turkey*, App. No. 48226/10 and 14027/11, CE:ECHR:2015:1201JUD004822610, judgment of 5 December 2015, para 52; ECtHR, *Vladimir Kharitonov v. Russia*, App. No. 10795/14, CE:ECHR:2020:0623JUD001079514, judgment of 23 June 2020, para 33.

⁵¹ *Ibid.*

⁵² *Ibid.*

⁵³ Case C-401/19, *Poland*, para 47.

that “[s]uch a prior review and prior filtering are liable to restrict an important means of disseminating online content and thus to constitute a limitation on the right guaranteed by Article 11 of the Charter”.⁵⁴

However, judges, clearly re-using parts of the Advocate General’s Opinion, held that Article 17 does not constitute a violation of the *essence* of Article 11 CFR.⁵⁵ While the provision does not “define the actual measures” that must be adopted, there are at least two unambiguous provisions (Articles 17(7) and (9)) stating that blocking of legitimate material cannot result from its application. This prescription of a specific result is, according to the Court, stronger than other parts of the provision that only require “best efforts”.⁵⁶ Article 17 thus requires “strict targeting” of the filtering “without thereby affecting users who are lawfully using those providers’ services”.⁵⁷ As a form of prior restraint, the legislation must be nevertheless subject to a “tight legal framework”.⁵⁸

Proportionality review

The Court thus turns its primary attention to the review of proportionality under Article 52(1) CFR.⁵⁹ It positions the interpretative balancing as a conflict between the provider’s right to conduct business (Article 16 CFR), users’ freedom of expression and information (Article 11 CFR), and the need to protect intellectual property (Article 17(2) CFR).⁶⁰ The starting point under any validity challenge, according to the Court, is that “an EU measure must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter”.⁶¹ This means that as long as the wording of a provision can be (re)balanced through the interpretation, the Court will not invalidate it.

Eventually, this suggests what happens in this case. The Court comes up with a restrictive reading of the scope of the obligatory filtering, which in turn releases the pressure on minimum EU procedural safeguards against abuse. As a result, the provision of EU law survives scrutiny.

Before proceeding to the proportionality review, however, the Court stresses that its assessment is limited to the questions of the *Union-wide validity* of a provision of an EU Directive with the EU Charter, and does not preclude follow-on constitutional assessments of its implementations in the Member States.⁶² This suggests that while the Court’s analysis eventually shows that the *EU legislature did enough* to strike a fair balance, it does not mean that the national legislatures cannot be expected to do more to reach the desired outcomes demanded by the Court’s ruling.

CJEU finds that even though the filtering measures must be derived from the provision’s purpose⁶³ and are not explicitly mentioned in it, the interference is sufficiently prescribed by the law. Court points out

⁵⁴ Case C-401/19, *Poland*, para 55.

⁵⁵ Case C-401/19, *Poland*, paras 76-81.

⁵⁶ Case C-401/19, *Poland*, para 78 (see also AG Opinion in Case C-401/19, *Poland*, para 207).

⁵⁷ Case C-401/19, *Poland*, para 81.

⁵⁸ Case C-401/19, *Poland*, para 68.

⁵⁹ Case C-401/19, *Poland*, para 82.

⁶⁰ Case C-401/19, *Poland*, paras 75 and 82.

⁶¹ Case C-401/19, *Poland*, para 70.

⁶² Case C-401/19, *Poland*, para 71.

⁶³ Case C-401/19, *Poland*, para 73.

that the area is subject to fast technological change and that ECtHR accepts even legislation “formulated in terms which are sufficiently open to be able to keep pace with changing circumstances”.⁶⁴

Article 17 also follows a legitimate objective and is also “necessary” to meet the need to protect IP rights at stake.⁶⁵ Alternatives to Article 17, so the Court, are “less effective” in terms of protecting the IP rights as those adopted by the EU legislature.⁶⁶ At the same time, it notes that even its judicial re-interpretation of Article 17 does *not* offer perfect preventive protection against repeated copyright infringements,⁶⁷ which is in line with the fact that IP rights and their protection is not absolute.⁶⁸

Finally, the Court reviews the proportionality of Article 17 in a strict sense. It notes that obligations imposed on providers do *not* disproportionality restrict the right to freedom of expression of users because they can be interpreted as largely aligned with the notion of strict targeting.⁶⁹

Relying on two result-oriented obligations to avoid over-blocking of legitimate material, and partly its earlier case law, the Court postulates the following *overarching requirement* for any filtering system:⁷⁰

“a filtering system which might not *distinguish adequately between unlawful content and lawful content*, with the result that its introduction could lead to the blocking of lawful communications, would be incompatible with the right to freedom of expression and information, guaranteed in Article 11 of the Charter”

This language is borrowed from *Sabam* and *Scarlet Extended* rulings.⁷¹ The Court continues the review by invoking various components of Article 17, such as mandatory exceptions and limitations, an obligation to inform users about them, the need to submit relevant information to trigger filtering obligations and prohibiting general monitoring-type filtering.⁷² The Court uses the prohibition of general monitoring obligation (Article 17(8)) to emphasize yet an additional requirement that any filtering system must fulfil. Drawing a parallel to its case-law on injunctions against intermediaries, the Court holds that Article 17(8) provides an “additional safeguard”.⁷³

“That clarification means that the providers of those services cannot be required to prevent the uploading and making available to the public of content which, in order to be found unlawful, would require an independent assessment of the content by them in the light of the information provided by the rightholders and of any exceptions and limitations to copyright.”

⁶⁴ Case C-401/19, *Poland*, para 74.

⁶⁵ Case C-401/19, *Poland*, para 83.

⁶⁶ Case C-401/19, *Poland*, para 83.

⁶⁷ Case C-401/19, *Poland*, para 91.

⁶⁸ Case C-401/19, *Poland*, para 92.

⁶⁹ Case C-401/19, *Poland*, paras 84 and 85.

⁷⁰ Case C-401/19, *Poland*, para 86 (emphasis mine).

⁷¹ Case C-70/10, *Scarlet Extended*, para 52 (“that injunction 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.”). The same standard was repeated in Case C-70/10, *Sabam*, para 50.

⁷² Case C-401/19, *Poland*, paras 87-90.

⁷³ Case C-401/19, *Poland*, para 90 (similarly, AG Opinion in Case C-401/19, *Poland*, para 195 ff.).

The Court here postulates a standard of technological configuration under which only filtering that can *autonomously* make the right calls between infringements and lawful content can be mandated. Unlike strict targeting, which is always constitutionally required, the standard of automatability only applies “in addition” if it is invoked by the EU legislature by reference to the prohibition of general monitoring.

The requirement of automatability of assessment speaks to questions of technological maturity and how much is delegated to autonomously decide by machines. It further narrows down the general holding according to which any filtering system must distinguish adequately between unlawful content and lawful content, by adding “on its own”. This additional requirement makes it clear that Article 17, and for that matter any other law invoking the prohibition of general monitoring obligations, may not require that legal false positives caused by an over-inclusive filtering system are mitigated by armies of human content moderators. In fact, the Court subsequently points to Recital 66 to establish that in such cases (when technology is not up to the task), right holders might still be required to notify infringements themselves.⁷⁴

The Court thus rejects AG’s proposal to read the case law as meaning that under “independent assessment”, humans and machines can together review the “matches” to achieve their “strict targeting”. The Court’s approach is “machine-only”. This could be explained by the fact that the Court also opted for a broader reading of the filtering mandate. While AG only proposed such application to instances involving “slavish” and “quasi-slavish” copies of works,⁷⁵ the Court did not limit the filtering to identical and equivalent content and focused entirely on the effects of technology at stake. Thus, while the Court gives, it also takes away. The net outcome for the right holders thus seems to depend on the maturity of available technologies and the granularity of their configuration in practice. The judicial standard, if well supervised, acts as an incentive to improve. The more precise the technology and its configuration, the more it ought to be used by relevant services.

	The Advocate General	The Court
Goal	Filtering must adequately distinguish legal and illegal content	
Scope	Only identical or equivalent infringements	Any infringements
Standard	Machine corrected by humans	Machines acting autonomously

Safeguards

In the very last step, the Court reviews the existence of the ex-post procedural safeguards for instances of blocking of lawful material. This part should be read together with the Court’s reminder that “[i]n addition, in order to satisfy the requirement of proportionality, the legislation which entails an interference with fundamental rights must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards”.⁷⁶ The goal is that “the persons whose exercise of those rights is limited have sufficient guarantees to protect them effectively against the risk of abuse”.⁷⁷ Moreover, “[t]he need for such safeguards is all the greater where the interference stems from an automated process”.⁷⁸

⁷⁴ Case C-401/19, *Poland*, para 91.

⁷⁵ AG Opinion in Case C-401/19, *Poland*, footnote 244.

⁷⁶ Case C-401/19, *Poland*, para 67.

⁷⁷ *Ibid.*

⁷⁸ *Ibid.*

The Court highlights that Article 17 includes provisions about a) effective and expeditious complaint and redress mechanism, b) out-of-court redress mechanism,⁷⁹ c) effective judicial remedies,⁸⁰ d) the existence of the stakeholder dialogue, and the ability of the European Commission to issue guidance.⁸¹ These ex-post safeguards, along with a re-interpretation of the material scope of Article 17, lead to the conclusion that the interference “has been accompanied by appropriate safeguards by the EU legislature”.⁸²

At the very end of the judgment, the Court cautions that the Member States cannot rely on the text of the Directive if its actual effects do not follow the fair balance. The overall balance crafted by the EU legislature is to be internalised by the Member States, which must “take care to act on the basis of an interpretation of that provision which allows a fair balance to be struck between the various fundamental rights protected by the Charter”.⁸³ The Member States must not only interpret their national law in a manner consistent with CJEU’s interpretation but have to refrain from acting on the basis of a conflicting interpretation.⁸⁴

Comments

The Grand Chamber judgment is, without a doubt, CJEU’s most significant digital speech ruling to date. Hidden in its complex context are valuable lessons.

Constitutional lessons

The first lesson concerns the quality of EU law-making. The Court uses its insights from data protection cases⁸⁵ to stress that the EU legislature has not only an obligation to formulate legislation that is proportionate, but “in addition”, its legislation must have “clear and precise rules governing the scope and application of the measure” and be equipped with “minimum safeguards” to prevent abuse.

The ruling requires that Union-wide safeguards are included in any piece of EU legislation that instigates an interference with the fundamental rights of EU citizens. The validity of EU legislation thus cannot be conclusively defended by pointing to the fact that the Member States can still fix all their human rights shortcomings on the Union legislation.

In 1989, in *Wachauf*,⁸⁶ the Court insisted that invalidity challenge must fail when the Community legislation “leave[s] the competent national authorities a sufficiently wide margin of appreciation to enable them to apply those rules in a manner consistent with the requirements of the protection of

⁷⁹ Case C-401/19, *Poland*, para 94.

⁸⁰ Case C-401/19, *Poland*, para 95.

⁸¹ Case C-401/19, *Poland*, para 96.

⁸² Case C-401/19, *Poland*, para 98.

⁸³ Case C-401/19, *Poland*, para 99.

⁸⁴ *Ibid.*

⁸⁵ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd*, paras 54 and 55 - based on Opinion of AG Villalón, *Digital Rights Ireland Ltd*, C-293/12 and C-594/12, ECLI:EU:C:2013:845, para 120 ([The EU legislature] 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.); see also Opinion 1/15, ECLI:EU:C:2016:656, paras 39, 140, 141; Case C-311/18, *Facebook Ireland and Schrems*, ECLI:EU:C:2020:559, paras 176, 180, 184; Joint Cases C-511/18, C-512/18 and Case C-520/18, *La Quadrature du Net and Others*, ECLI:EU:C:2020:791, para 132; Case C-623/17, *Privacy International*, ECLI:EU:C:2020:790, para 68.

⁸⁶ Case Case 5/88, *Hubert Wachauf*, ECLI:EU:C:1989:321, para 22.

fundamental rights”.⁸⁷ *Wachauf* was described as indicating decentralised review by the national courts.⁸⁸ After the adoption of the EU Charter, *Test-Achat* (2011) case showed the opposite tendency. The Court held that the EU legislature drafted too broad a derogation from a right to equal treatment between men and women as the derogation could last indefinitely and was not subject to other meaningful scope limits. The Court invalidated the exception in a Directive arguing that “there is a risk the EU law may permit [the interference] to persist indefinitely” which makes it incompatible with the EU Charter.⁸⁹ The case, in contrast to *Wachauf*, emphasized a centralised review of the validity.⁹⁰

To give this development some context, before *Test-Achat* (2011) and *Digital Rights Ireland* (2014), the Court was often criticised for a weak standard and very low willingness to invalidate provisions of the secondary EU law, including EU Directives. Damien Chalmers’s critique from 2010 captures this well:⁹¹

Moreover, it is very difficult to find many Union legislative measures that have been struck down for violation of fundamental rights. No Directive, for example, has ever been struck down by the Court on those grounds. Judicial intervention is rare. Another hallmark is an unpredictable and weak standard of review. In difficult cases, the Court of Justice has either enunciated the basic rights and indicated the matter to be exclusively one for the national court or simply deferred to the national constitutional settlement.

Poland v Council/Parliament shows that the Court’s standard of review is gradually tightening. It disciplines the EU legislature by requiring *minimum* Union-wide safeguards.⁹²

According to the Court, in the case of Article 17, the EU legislature did just enough to introduce ex-post safeguards, which were seen as sufficient to cope with the instances of over-blocking. The Court cleverly relieved the pressure on the existence of these safeguards by narrowing the number of instances in which

⁸⁷ Case Case 5/88, *Hubert Wachauf*, ECLI:EU:C:1989:321, paras 22, 23. See the commentary on this ruling by several authors in Luis Miguel Poiares Pessoa Maduro and Loïc Azoulai (Ed.), *The Past and Future of EU Law: The Classics of EU Law Revisited on the 50th Anniversary of the Rome Treaty* (Bloomsbury 2010).

⁸⁸ Zdeňek Kühn, *Wachauf and ERT: On the Road from the Centralised to the Decentralised System of Judicial Review* in Luis Miguel Poiares Pessoa Maduro and Loïc Azoulai, *The Past and Future of EU Law: The Classics of EU Law Revisited on the 50th Anniversary of the Rome Treaty* (Bloomsbury 2010), p 151.

⁸⁹ Case C-236/09, *Association Belge des Consommateurs Test-Achats and Others*, ECLI:EU:C:2011:100, para 21, 31 and 32.

⁹⁰ A brief preview of leading cases concerning validity challenges of EU Directives on the basis of fundamental rights: Case C-236/09, *Association Belge des Consommateurs Test-Achats and Others*, ECLI:EU:C:2011:100 (EU Directive; partly invalid); Case C356/12, *Glatzel*, ECLI:EU:C:2014:350 (EU Directive; valid); Case C-200/96, *Metronome Musik*, ECLI:EU:C:1998:172 (EU Directive; valid); Case C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert*, ECLI:EU:C:2010:662 (EU Regulation; partly invalid); Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd*, ECLI:EU:C:2014:238 (EU Directive; fully invalid); Case C-291/12, *Michael Schwarz*, ECLI:EU:C:2013:670 (EU Regulation; valid); Case C-283/11, *Sky Österreich*, ECLI:EU:C:2013:28 (EU Directive; valid).

⁹¹ Damian Chalmers, “Looking Back at ERT and its Contribution to an EU Fundamental Rights Agenda” in Luis Miguel Poiares Pessoa Maduro and Loïc Azoulai (Ed.), *The Past and Future of EU Law: The Classics of EU Law Revisited on the 50th Anniversary of the Rome Treaty* (Bloomsbury 2010), p. 142.

⁹² See for analysis of this question: Opinion of AG Villalón, *Digital Rights Ireland Ltd*, C-293/12 and C-594/12, ECLI:EU:C:2013:845, para 120.

they will be needed. It did so by narrowing down the mandated use of filtering tools.⁹³ The Court's review thus did not respond by invoking the Member States as solely responsible. Instead, it was ready to accept that the EU legislature must, to a limited degree, police the risk that it creates. Thus, the judicial review is not entirely decentralised even for what remains in the room for implementation.

CJEU's explicit recognition of minimum Union-wide safeguards is very important and needed. That being said, as a principle, it must be applied carefully.

On one hand, the political economy of the EU legislative process invites that when far-reaching proposals limiting fundamental rights are being discussed, it is (politically) easier to leave safeguards unaddressed and ask the national legislatures to fix this gap in course of their national implementations. However, when the European Union legislature, despite the competence limits, at once bears some central responsibility for designing the safeguards and cannot simply leave their design to the Member States, this pressures the EU legislature to pass better Union legislation. It shifts away from decentralised validity reviews of its national implementations to the central Union-wide review of minimum safeguards. The concept basically says that it is not always conclusive whether the EU legislation can be implemented by the Member states in a fundamental rights-compliant way in their domestic legal order. Any centralised review *apriori* suspects the national legislatures from not being able to observe fundamental rights. To some extent, this is surely justified, but one can imagine it going too far too. Too centralised review shifts power to the CJEU and presupposes a more uniform idea of fundamental rights.⁹⁴ As noted by Kühn, „[i]t eliminates, in a greater number of cases, the need to set aside or nullify European rules which could operate in conflict with fundamental rights on the local level via their national application“.⁹⁵ Ultimately, it politically constrains the incomplete consensus within secondary EU law that the EU measures such as EU Directive were set to facilitate.

The ruling shows that the Court is mindful of only requiring “minimum safeguards”. The Advocate General highlighted a number of other appropriate safeguards that are missing, such as state *supervision* of the filtering measures. The Court does not mention supervision or these other safeguards at all. There are two ways how to read this omission. Either the Court disagreed that supervision and other missing safeguards are not crucial at all, or it did not think that they shall be part of the minimum that the EU legislature should have delivered.⁹⁶ The more so that the Court itself notes that its review of Article 17, as a provision of an EU directive, should not be prejudicial to those national reviews. If we read the ruling in light of the AG's Opinion, then it is likely that the Court only agreed with the AG that such supervision and other safeguards simply do not have to be part of EU law, but still must be addressed on the national level.

Finally, the Court postulates a clear principle that the states are responsible for the failings of firms which they expect to act to enforce the law. Such “delegated enforcement” is attributable to the state, and the state, including the legislature, cannot disclaim its responsibility for the day-to-day working of the system

⁹³ The irony of history is that these safeguards were inserted at the last minute of the legislative process by the critics of the provision. Thus, the life support to Article 17 came from its opponents.

⁹⁴ Zdeňek Kühn, “Wachauf and ERT: On the Road from the Centralised to the Decentralised System of Judicial Review” in Luis Miguel Poiarés Pessoa Maduro and Loïc Azoulai (Ed.), *The Past and Future of EU Law: The Classics of EU Law Revisited on the 50th Anniversary of the Rome Treaty* (Bloomsbury 2010), p. 153.

⁹⁵ *Ibid.*

⁹⁶ This is an aspect that would have been likely be thematised by future challenges to national implementations. But as is noted below, the DSA somehow mitigates the problems.

that it helps to establish through its legislation. The state is responsible for a measure that is implemented in response to incentives that it sets in the legislation, regardless of whether those measures are named in it or not. If only incentives are embodied in the law, the Court will review their likely real-world effects, and analyse them, even though factual evidence of the exact implementation might be missing.

Digital policy lesson

The second lesson concerns fundamental rights in the context of automated decision-making. The ruling adds an additional building block to its growing case law concerning the practice.

In the present case, automated decision-making (ADM) consisted of preventive blocking of content on platforms by filters. According to the Court, such ADM is only possible when it is ‘strictly targeted’ to unlawful material. Filters which are configured for use cases in which they fail to ‘adequately distinguish’ lawful and unlawful, cannot be trusted, regardless of other (usually ex-post) safeguards. EU law mandating such ‘inadequate’ filters would violate freedom of expression. ‘Strict targeting’ thus represents the overarching constitutional limit for any ADM system that implicates the right to freedom of expression.

Only if the EU legislature invokes the prohibition of general monitoring,⁹⁷ the technology must, in addition, be able ‘autonomously capable of such strict targeting. If the law does not stipulate this additional safeguard, it can include humans to resolve false positives. This differentiation is very intuitive. The ultimate constitutional standard is to adequately avoid making mistakes. The prohibition of general monitoring obligation, on the other hand, was meant to prevent demands that providers apriori review the content posted on their platforms. It protects users, their speech and privacy interests, and providers, their business and speech interests, alike. While the Court narrowed down the statutory concept over the years to absorb new capabilities of automation,⁹⁸ the original core use case remained the same: at the very least, it shall prevent lawmakers from asking providers to employ people to manually and proactively check the content on their service. If the Court narrows down the standard further from “machine-only” stance, any added value compared to the constitutional requirement of ‘strict targeting’ is lost, and the provision becomes superfluous.

To demonstrate this, consider the currently pending proposal to fight child abuse material through an EU Regulation. The European Commission proposed to require on-device scanning of chats to detect and filter away child abuse material relying on self-learning artificial intelligence systems.⁹⁹ The systems employed should mitigate false positives through joint human review of matches by state authorities and providers.¹⁰⁰ After the present judgment, such a system could survive Article 11 CFR scrutiny only if it can adequately distinguish between lawful and unlawful material and put in place sufficient safeguards against abuse. Unless the law will try to invoke general monitoring prohibition, Article 11 CFR on its own shall not prevent reliance on human moderators per se to help to avoid false positives. That is the qualitative difference which the general monitoring obligations prohibition introduces.

⁹⁷ Folkert Wilman, “Two emerging principles of EU internet law: A comparative analysis of the prohibitions of general data retention and general monitoring obligations” (2022) 46 Computer Law & Security Review, 1-18.

⁹⁸ AG Opinion in Case C-401/19, *Poland*, paras 110 to 113.

⁹⁹ See Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (2022) COM/2022/209 final.

¹⁰⁰ See more about the plans: <<https://netzpolitik.org/2022/geleakter-bericht-eu-kommission-nimmt-hohe-fehlerquoten-bei-chatkontrolle-in-kauf/>>

To summarize this, if the prohibition of general monitoring obligation is not invoked, the legislature must assure its strict targeting. Such strict targeting does not have to result only from the decision-making by machines. Most notably, it can be supplemented by humans. However, if it invokes such statutory prohibition, the Court conceptualizes it as “an additional” safeguard. Only then, the appropriateness of a technological solution must be judged by the quality of what it can do *autonomously*. As a result, the authorities cannot demand that those who implement the filters simply improve on them by employing armies of human content moderators. The automatability limit applies not only to Article 17 of the Copyright DSM Directive but also to any preventive measures issued by national authorities in the context of the upcoming Digital Services Act,¹⁰¹ e.g., as injunctions against intermediaries in IP law.

At the same time, any automated system that desires to offer an appropriate accuracy rate might implicate other fundamental rights, such as the right to privacy and data protection, in the way of doing so. Thus, even *if* the manual review of matches of messages in chats might need to be done to satisfy Article 11 CFR, it might for that very reason violate Articles 7 and 8 CFR as a such review of messages can intrude deeply into people’s personal sphere. This is clear from another Grand Chamber judgment, *Ligue des droits humains*, handed down just a couple of months later. There, the Court rejected that an EU Directive prescribing the collection of passenger data in the context of air travel to fight terrorism could be interpreted as allowing assessment by “artificial intelligence” using “self-learning systems”.¹⁰² Such systems, in the Court’s view, are “capable of modifying without human intervention or review the assessment process”.¹⁰³ As a result, “given the opacity which characterises the way in which artificial intelligence technology works, (...) use of such technology may deprive the data subjects also of their right to an effective judicial remedy”.¹⁰⁴ The constitutional limits imposed by these three provisions of the EU Charter cumulatively are thus much stricter, as they jointly only allow ADM that fulfil all three standards at the same time.

Copyright lessons

Finally, the ruling offers several lessons for EU copyright debates.

By its conceptualisation of Article 17(1) as a “new specific liability mechanism” that is distinct from the general regime,¹⁰⁵ the Court agreed with the Advocate General about the law granting copyright holders expectations that did not exist before. The Court thus subscribed to the idea of a special regime, which is distinctly separate from Article 3 of the InfoSoc Directive.¹⁰⁶

¹⁰¹ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

¹⁰² Case C-817/19, *Ligue des droits humains v. Conseil des ministres*, ECLI:EU:C:2022:491, para 194.

¹⁰³ *Ibid.*

¹⁰⁴ Case C-817/19, *Ligue des droits humains*, para 195.

¹⁰⁵ Case C-401/19, *Poland*, paras 30, 31 and 32.

¹⁰⁶ Martin Husovec and Joao Pedro Quintais, “How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms under the Copyright in the Digital Single Market Directive” 70(4) *GRUR International* (2021), 325–348 (discussing this as options C and D). On the different views before the judgment, see Matthias Leistner, “European Copyright Licensing and Infringement Liability Under Article 17 DSM-Directive Compared to Secondary Liability of Content Platforms in the U.S. – Can We Make the New European System a Global Opportunity Instead of a Local Challenge?” (2020) 2 *Zeitschrift für Geistiges Eigentum/Intellectual Property Journal* (ZGE/IPJ), 123-214; Jan Bernd Nordemann and Julian Wiblinger, “Article 17 DSM-RL – Spannungsverhältnis Zum

The Court also clearly supported the thinking behind the widely discussed German implementation of Article 17.¹⁰⁷ German law foresees legislative thresholds for what can be expected to be automated. This was criticised as going beyond the text of the directive. However, based on the judgment, as long as the thresholds are technologically sound, the German implementation is not only fully compatible with EU law but is clearly embodying the spirit of the Court's judgment. Matthias Leistner summarised it better than I possibly can:¹⁰⁸

“Thus, the German solution not only passes the compliance test under Art. 5 InfoSoc Directive and Art. 17 but is now a genuine example for the implementation of Art. 17 in conformity with EU constitutional law in other Member States. It is somewhat paradoxical, however, that Member States which have implemented Art. 17 literally now have to fear that their implementation is not in line with the Charter, while Art. 17 itself is proportional.”

Only if it can be shown that German law excludes from automation, through its legislative thresholds, what can be adequately automated, it is in violation of EU law. The Court's requirement that technology must be capable of autonomous assessment without human intervention gives a strong boost to the German legislature's initial intention to distinguish between assessment of infringements that are “machine-eligible” and “non-eligible”.¹⁰⁹

The CJEU also clearly provided ammunition to citizens of those Member States whose legislatures thought that copying and pasting the provision without creating functioning safeguards against over-blocking is possible. Such implementations can be now reviewed against their compatibility with the EU law and national constitutions. The obvious candidates for missing safeguards are transparency, state supervision, effective sanctions, and provisions against abuse. But before the next stage of debates could even start, the EU legislature introduced them through horizontal legislation. The additional safeguards that the Court did not require from the EU legislature, such as transparency of algorithms, concrete design of the dispute settlement, or collective redress for content creators, can now be largely found in the upcoming Digital Service Act.¹¹⁰

The DSA will apply horizontally and as of 17 February 2024, will supersede any national implementations of Article 17 concerning explanation, contestation of decisions and transparency.¹¹¹ While Article 17 will

Bisherigen Recht?“ (2020) GRUR 569; Eleonora Rosati, “Five Considerations for the Transposition and Application of Article 17 of the DSM Directive” (2021) 16(3) *Journal of Intellectual Property Law & Practice*, 265-270.

¹⁰⁷ See Articles 9 and 10 of the German implementing law: Gesetz über die urheberrechtliche Verantwortlichkeit von Diensteanbietern für das Teilen von Online-Inhalten (Urheberrechts-Diensteanbieter-Gesetz – UrhDaG, 2021).

¹⁰⁸ Matthias Leistner, “The Implementation of Art. 17 DSM Directive in Germany – A Primer with Some Comparative Remarks” (2022) 71(10) *GRUR International*, 909-923, 918.

¹⁰⁹ See Articles 5 and 6 of the proposal of the German implementing law, available here: https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/DiskE_II_Anpassung%20Urheberrecht_digitaler_Binnenmarkt.pdf?__blob=publicationFile&v=2. For a similar concept, see Martin Husovec, “The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown? Which is Superior? And Why?” (2018) 42(1) *Columbia Journal of Law & the Arts*, 53-84 (discussing automatable-infringements (A-Types) vs not-yet-automatable infringements (NYA-Types)).

¹¹⁰ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act - DSA)

¹¹¹ See for more discussion Joao Quintais and Sebastian Schwemer, “The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?” (2022) 13(2) *European Journal of Risk Regulation*, 191-217. doi:10.1017/err.2022.1

constitute *lex specialis* as the only law mandating the use of filters in the EU, once filters are used, any false positives will be offered safeguards of the DSA. The automated decisions will be accompanied by explanations,¹¹² subject to internal and external dispute resolution,¹¹³ and far-reaching transparency obligations.¹¹⁴ Consumer associations will be able to assist content creators and sue on behalf of their users to enforce these obligations.¹¹⁵ The same rules will also benefit the rights holders.

But the most interesting development is that the line the Court tries to draw in the judgement between adequate and inadequate filters will be often drawn by tools incorporated in the DSA. Very large online platforms will have to conduct risk-mitigation assessments on filters mandated by Article 17 CDSMD.¹¹⁶ If these assessments show significant shortcomings, the DSA doubles down on Article 17(7)'s obligation to refrain from using them. For very large online platforms, the use of such inadequate filters becomes a question of DSA compliance. As with any other issue, it can be enforced through private and public enforcement measures that are enabled by the DSA. For OCSSPs who are not VLOPs, the milder version of diligence comes through transparency rules.¹¹⁷ Their filtering tools and configuration will be subject to transparency obligations, including disclosure of what systems are used, what are their error rates and what safeguards are used to mitigate the mistakes.¹¹⁸ Thus, all OCSSPs who are at least medium-sized enterprises must at least assure compliance through their suppliers of filtering technologies. The obligations are thus likely to trickle down the supply chain. Thus, with the DSA, additional safeguards envisaged by the Advocate General, and implicitly expected by the Court, arrive at last in all the Member States of the European Union.

Conclusion

András Sajó, a former Hungarian judge of the European Court of Human Rights, once wrote that „constitutional tribunals have more of a chance to provide lasting and unsupervised determinations of the law by interpreting the law rather than voiding it“.¹¹⁹ *Poland v Council/European Parliament* will undoubtedly become one of those silent building blocks of European digital constitutionalism. What *Digital Rights Ireland* did for privacy and data protection issues, this Grand Chamber ruling is likely to do for people's freedom of expression.

CJEU's judgment in *Poland v Council and European Parliament* is impressive in many regards and serves as a testimony of the Court's strength in dealing with complicated issues of the digital policy if the framing is right. It shows that Luxembourg judges are more than willing to closely follow Strasbourg jurisprudence and develop it further for EU citizens. Finally, the ruling also suggests that political might and sensitivity of copyright and data protection law will continue to shape our digital civil liberties for the years to come. The good news for Europeans is that CJEU is tightening the grip on its standard of review of EU legislature's acts and showing a willingness to tackle new challenges on both fronts.

¹¹² Article 17 DSA.

¹¹³ Articles 20 and 21 DSA.

¹¹⁴ Articles 15, 24, 39, 42 DSA.

¹¹⁵ Articles 86 and 89 DSA.

¹¹⁶ Article 34 DSA.

¹¹⁷ Article 15(1)(e) DSA.

¹¹⁸ Article 15(1)(e) DSA.

¹¹⁹ András Sajó, "Constitutional Adjudication in Light of Discourse Theory" (1995) 17 *Cardozo Law Review*, 1193-1229, 1208.

Author's declaration: This annotation has not been published, nor is its publication pending or under consideration elsewhere.