Received: 6 October 2023 | Accepted: 9 October 2023

DOI: 10.1111/eulj.12475

VARIETY: ORIGINAL ARTICLE

WILEY

Taking fundamental rights seriously in the Digital Services Act's platform liability regime

Giancarlo Frosio | Christophe Geiger*

Abstract

This article highlights how the EU fundamental rights framework should inform the liability regime of platforms foreseen in secondary EU law, in particular with regard to the reform of the E-commerce directive by the Digital Services Act. In order to identify all possible tensions between the liability regime of platforms on the one hand, and fundamental rights on the other hand, and in order to contribute to a well-balanced and proportionate European legal instrument, this article addresses these potential conflicts from the standpoint of users (those who share content and those who access it), platforms, regulators and other stakeholders involved. Section 2 delves into the intricate landscape of online intermediary liability, interrogating how the E-Commerce Directive and the emerging Digital Services Act grapple with the delicate equilibrium between shielding intermediaries and upholding the competing rights of other stakeholders. The article then navigates in Section 3 the fraught terrain of fundamental rights as articulated by the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) under the aegis of the European Convention on Human Rights and the EU Charter. This section poses an urgent inquiry: can the DSA's foundational principles reconcile these legal frameworks in a manner that fuels democracy rather than stifles it through inadvertent censorship? Section 4 then delves into the intricate relationship between fundamental rights and the DSA reform. This section conducts a comprehensive analysis of the key provisions of the DSA, emphasising how they underscore the importance of fundamental rights. In addition to mapping out the strengths of the framework the section also identifies existing limitations within the DSA and suggests potential pathways for further refinement

* Giancarlo Frosio is a Professor of Intellectual Property and Technology Law and Director of the Global Intellectual Property and Technology (G-IPTech) Centre at the School of Law of Queen's University Belfast, Non-Resident Fellow at the Stanford Law School Center for Internet and Society, and Associate Faculty at the NEXA Center for Internet and Society; Christophe Geiger is Professor of law at the Luiss Guido Carli University in Rome (Italy), Global Visiting Professor of Law, New York University School of Law, US (Fall 2023) and President of the International Association for the Advancement of Teaching and Research in Intellectual Property (ATRIP). The authors are extremely grateful to Khrystyna Fedunyshyn, Doctoral Candidate at the University of Strasbourg, for her invaluable contribution in the completion of this research project. The authors would further like to thank Elena Izyumenko, Assistant Professor at the Institute for Information Law at the University of Amsterdam for her valuable comments on the draft. They are further deeply indebted to Frasier Simpson for outstanding editing support and Varnita Singh for excellent research support in early stages of the drafting of this study. Finally, the authors would like to thank Copyright for Creativity (C4C) for supporting this research project.

Funding information: Copyright for Creativity (C4C)

and improvement. This article concludes by outlining key avenues for achieving a balanced and fundamental rights-compliant regulatory framework for platform liability within the EU.

1 | INTRODUCTION: FUNDAMENTAL RIGHTS ONLINE AND PLATFORM LIABILITY IN THE EU

The activities of Digital Service Providers (DSPs)[1] in contemporary information societies raise a number of ethical, legal, and social challenges. Some DSPs are in a unique position to influence users' ability to access information and their interaction with it. DSPs thus fulfil *de facto* an important democratic function, acting as facilitators of users' speech, creativity and exchange of ideas.[2] At the same time, recent events have revived long-standing concerns regarding private ordering and the moderating powers available to global platforms. These powers are so pervasive that global platforms can dramatically shape political and cultural discourse. Take, for example, Twitter's permanent suspension of a sitting U.S. President's account without judicial or independent oversight.[3] Meanwhile, entrepreneurs without any democratic mandate stir controversy. It is sufficient to take the example of Elon Musk's acquisition of Twitter.[4] Moreover, Facebook's arbitrary censorship practices, which have included the banning of artworks like Michelangelo's *David* for violating its standards on nudity or sexual acts, as well as iconic documentary photos like the *Napalm Girl* from the Vietnam War and pictures of visible breastfeeding, reveals a disturbingly arbitrary approach to content moderation.[5] These events raise issues regarding platforms' liability, role, and regulation to a whole new level. Platforms can influence elections or change the course of events by silencing speech according to alleged infringements of their Terms of Service. While certain harmful content posted online requires intervention, it has been increasingly openly questioned whether platforms should alone be the ones to decide what is available online and what is not.[6]

This means that Fundamental Rights (FRs) protection is vital in any discussion regarding DSPs policy and their regulation, be it by intellectual property laws or by other legislative or judicial intervention.[7] Traditionally, intermediary and platform liability regulations have been struggling to find a proper balance between competing rights that might be affected by DSPs' activities and obligations.[8] Pristine approaches, reflected in the EU E-Commerce Directive (ECD), have established limited liability frameworks including exemptions for DSPs, which in turn provided

[1]This terminology, used throughout the article, does not imply any different connotation than traditional terms such as Information Society Service Providers, Internet Service Providers or Online Service Providers. It is only meant to match better the scope of the Digital Services Act. The notion of 'Digital Service Providers' includes at least three major categories of providers: access providers, hosting providers and search engines. However, more categories and sub-categories can be identified, and their identification remains in constant flux due to fast-paced technological development. For a taxonomical discussion of online intermediaries and service providers, see G. Dinwoodie, 'Who Are Internet Intermediaries?', in G. Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (OUP 2020) 37–56.

[2]See, e.g., N. Elkin-Koren and M. Perel, 'Guarding the Guardians: Content Moderation by Online Intermediaries and the Rule of Law', in Frosio (ed) (n 1) 669–678.

[3]See, e.g., Oversight Board upholds former President Trump's suspension, finds Facebook failed to impose proper penalty (*Oversight Board*, May 2021) <https://oversightboard.com/news/226612455899839-oversight-board-upholds-former-president-trump-s-suspension-finds-facebook-failed-to-impose-proper-penalty>.

[4]See, e.g., M. Zahn, 'A timeline of Elon Musk's tumultuous Twitter acquisition attempt' (*ABC News*, 13 July 2022) <https://abcnews.go.com/Business/timeline-elon-musks-tumultuous-twitter-acquisition-attempt/story?id=86611191>.

[5]See M. Loi, *Making sense of the Digital Services Act How to define platforms' systemic risks to democracy* (Algorithmic Watch, August 2023), 8 <https://algorithmwatch.org/en/wp-content/uploads/2023/08/AlgorithmWatch_Risk_Assessment-DSA.pdf>.

[6]See, e.g., the Speech by President of the European Commission von der Leyen at the European Parliament Plenary on the inauguration of the new President of the United States and the current political situation, Brussels, 20 January 2021, <https://ec.europa.eu/commission/presscorner/detail/en/speech_21_167> (noting that 'No matter how right it may have been for Twitter to switch off Donald Trump's account five minutes after midnight, such serious interference with freedom of expression should be based on laws and not on company rules. It should be based on decisions of parliaments and politicians and not of Silicon Valley managers').

[7]On the increasing influence of human and fundamental rights on the resolution of intellectual property (IP) disputes, see C. Geiger, 'Constitutionalising Intellectual Property Law?, The Influence of Fundamental Rights on Intellectual Property in Europe', (2006) 37(4) IIC 371; 'Fundamental Rights as Common Principles of European (and International) Intellectual Property Law', in A. Ohly (ed.), *Common Principles of European Intellectual Property Law* (Mohr Siebeck 2012) 223; 'Reconceptualizing the Constitutional Dimension of Intellectual Property - An Update', in P. Torremans (ed.), *Intellectual Property and Human Rights* (4th ed., Kluwer Law Int'l 2020) 117.

[8]See, e.g., for a discussion of the nexus between liability and balancing exercise, C. Angelopoulos and S. Smeth, 'Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability', (2017) 8(2) *Journal of Media Law*, 266–301 <https://www.ivir.nl/publicaties/download/Notice_and_Fair_Balance.pdf>.

strong safeguards for users' fundamental rights. In order to protect the ideal of a free internet—and maximise incentives for Internet entrepreneurs—policy makers decided initially to set up a legal framework that rejected any approach that turned online intermediaries into some kind of Internet police.[9]

Since then, governments and rightsholders have attempted to enlist intermediaries to cleanse the internet of allegedly infringing and illicit material.[10] Indeed, due to public enforcement authorities' lack of technical knowledge and resources to address an unprecedented challenge in terms of global human communications, the temptation is great to coactively outsource enforcement online to private parties. Private ordering—and the retraction of the public from online enforcement—does however convey an amorphous notion of responsibility that incentivises intermediaries' intervention to police themselves allegedly infringing activities on the internet. It highlights unescapable tensions with fundamental rights—such as freedom of information, freedom of expression, freedom of business or a fundamental right to internet access—by limiting access to information, causing chilling effects, or curbing due process.[11]

In discussions of content moderation on the internet, the focus often tilts towards the role of platforms and private actors, eclipsing the substantial and often insidious influence of States in shaping the digital landscape. While the existing discourse has often framed online content moderation as a function of privatised governance by platforms, it is also important to keep in mind that State-driven forces can compel platforms to operate in certain ways—ostensibly to protect citizens, but sometimes to enforce state-centric worldviews and curtail freedom of expression.[12] For instance, countries with more centralised governance structures, like China, have enacted policies enforcing pervasive control of online content and perpetuate state ideology.[13] In Europe, the recent trend has been towards imposing enhanced responsibilities on online platforms and a tighter regulatory approach.[14] Contrastingly, nations such as the United States have adopted a staunch "First Amendment absolutism",[15] vigorously safeguarding the interests of major tech conglomerates and digital platforms. While this approach aligns closely with domestic priorities, it often overlooks the potential collateral damage to competing fundamental rights that may be compromised by the unchecked presence of illicit content online. Interestingly, the approaches to intermediary liability regulation in China and the U.S. could be considered as representing opposite ends of the policy spectrum. With recent developments like the Digital Services Act (DSA),[16] the EU embraces a compromise, upholding the existing liability

[9]See, e.g., J. Boyle, Intellectual Property? Two Pasts and One Future, Information Influx International Conference, Amsterdam, 2–4 July 2014 <https://www.youtube.com/watch?v=gFDA-G_VqHo>.

[10]See, e.g., G. Frosio, 'Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility' (2017) 25 *Oxford JILIT*. 1–33.

[11]In this context, while beyond the purview of our review, it's pertinent to note legislation that restricts online news dissemination or services that facilitate links to news, as exemplified by art. 15 of the Directive 2019/790/EU of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L 130/92 and the Canadian Online News Act, Bill C-18 of 22 June 2023 (imposing a mandate that restricts individuals in Canada from viewing or disseminating news articles and multimedia content posted by news outlets via platforms like Facebook and Instagram). See also C. Geiger, G. Frosio and O. Bulayenko, 'The Introduction of a Neighbouring Right for Press Publisher at EU Level: The Unneeded (and Unwanted) Reform', (2017) 34(2) *European Intellectual Property Review*, 202–210 (emphasising how the reform might lead to less news availability and re-centralisation of the market for news).

[12]For further examples that could be relevant to this discussion, consult the AIDV Index. Notably, see Brazil on page 161, Singapore on pages 858–859, and Thailand on page 965. The AIDV Index is accessible at: https://www.caidp.org/reports/aidv-2022.

[13]See Internet Information Service Algorithmic Recommendation Management Provisions, Effective 1 March 2022 (translated by Rogier Creemers, Graham Webster and Helen Toner), art. 1, <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022>.

[14]See, e.g., European Commission Communication, 'Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms' COM(2017) 555 final, s. 6 (noting 'the constantly rising influence of online platforms in society, which flows from their role as gatekeepers to content and information, increases their responsibilities towards their users and society at large'). See also G. Frosio and M. Husovec, 'Accountability and Responsibility of Online Intermediaries' in G. Frosio, see n. 1, 613–630; G. Frosio, see n. 10, 1–33; M. Husovec, *Injunctions against Intermediaries in the European Union: Accountable but Not Liable?* (CUP 2017).

[15]See, e.g., Communication Decency Act, § 230. See also, recently leaving intact immunity under CDA § 230 in suits sought to hold Twitter and Google liable for terror content, Twitter, Inc. v. Taamneh, 598 U.S. 471 (2023) and Gonzalez v. Google LLC, 598 U.S. 617 (2023).

[16]See Regulation 2022/2065/EU of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 OJ L 277/1 (hereafter "DSA"). The DSA has been published in the Official Journal as of 27 October 2022 and came into force on 16 November 2022. The DSA will be directly applicable across the EU and will apply to all in-scope service providers by 17 February 2024, although VLOPs and VLOSEs are required to comply with the new rules by no later than 1 September 2023. For full commentary on the DSA, see F. Hofmann and B. Raue (eds), *Digital Services Act* (Nomos 2023) (an English version is announced for early 2024); T. Kraul (ed), *Das neue Recht der digitalen Dienste* (Nomos 2023); M. Husovec and I. Roche Laguna, *Principles of the Digital Services Act* (Oxford University Press, forthcoming 2023), with a short primer of the book and the DSA available at M. Husovec and I. Roche Laguna, 'Digital Services Act: A Short Primer' (2022) SSRN Research Paper no. 4153796/22 <https://ssrn.com/abstract=4153796>. On spillover effect of the DSA for the rest of the world, see, D. Keller, 'The EU's new Digital Services Act and the Rest of the World' (*Verfassungsblog*, 7 November 2022) <https://verfassungsblog.de/dsa-rest-of-world>.

exemption/safe harbour regime, while implementing more institutionalised, stringent oversight of digital platforms' content moderation and operational activities. This move ostensibly aims to enhance user protection and transparency, as well as to serve broader societal objectives. While emphasising citizen welfare over state control, when compared to the U.S. model, the EU approach places less emphasis on market self-regulation and privileges a regulatory, more interventionist approach over private ordering.

One mechanism that is becoming increasingly prevalent in this dynamic is what has been dubbed the 'invisible handshake' between public and private entities.[17] Here, the enhanced enforcement measures that online intermediaries voluntarily adopt are often not solely private decisions but are shaped, nudged, or even coerced by public deal-making. Because platforms are afforded certain liability safe harbours, they gain significant control over user-generated content. However, as Rebecca Tushnet pointedly describes, they wield this "power without responsibility", lacking any accountability to uphold their users' speech rights.[18] This lack of accountability towards user rights creates a vacuum that governments are more than willing to fill by exerting pressure on platforms to remove content.[19] While seemingly voluntary, this public deal-making has an economic justification: the avoidance of new and potentially restrictive regulations. The cost and uncertainty involved in resisting such governmental pressures serve as potent catalysts, making it financially sensible for platforms to comply. Derek Bambauer's work *Against Jawboning* provides an illustrative example, citing how Representative James Sensenbrenner pressured the US Internet Service Provider Association with the metaphor of a carrot and stick, essentially stating that voluntary compliance is preferable to punitive legislation.[20] Another stark example is the EU Code of Conduct for hate speech, which although aiming to counter hate speech, raises serious questions about due process, prior restraint, and the applicability of human rights safeguards.[21]

In addition, private ordering-based enforcement looks for an 'answer to the machine in the machine.'[22] By enlisting online intermediaries as "watchdogs", governments de facto however delegate online enforcement to algorithmic tools. Given the unsustainable transaction costs related to manual checking of illegal content, online intermediaries are forced to deploy algorithmic tools to perform monitoring and filtering, and limit their liability. In fact, content moderation online, including the moderation of intellectual property infringing content, defamatory content, dangerous and hate speech, child pornography and abuse, or online disinformation[23] – and the adjudication of disputes with and between users – have been increasingly dealt with through automated filtering and other algorith-

[17]Cf. M. Birnhack and N. Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment', (2003) 8 *Virginia Journal of Law and Technology*, 6.

[18]R. Tushnet, 'Power Without Responsibility: Intermediaries and the First Amendment', (2008) 76(4) *George Washington Law Review*, 986, 986.

[19]See ibid.; D. Keller, 'Who Do You Sue? State and Platform Hybrid Power over Online Speech', (2019) Aegis Series Paper no. 1902, <https://www.lawfareblog.com/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech>.

[20]See D. Bambauer, 'Against Jawboning', (2015) 100 *Minnesota Law Review*, 51, 51–52.

[21]See, e.g., E. Aswad, 'The Role of US Technology Companies as Enforcers of Europe's New Internet Hate Speech Ban', (2016) 1(1) *Columbia Human Rights Law Review Online*, 1, 6.

[22]See C. Clark, 'The Answer to the Machine is in the Machine' in P. B. Hugenholtz (ed), *The Future of Copyright in a Digital Environment* (Kluwer Law International 1996) 139 (discussing the application of digital right management systems to enforce copyright infringement online). For a criticism and a reply to Charles Clark, see C. Geiger, 'The Answer to the Machine should not be the Machine, Safeguarding the Private Copy Exception in the Digital Environment' (2008) 30 *EIPR* 121; C. Geiger, 'The Replacement of Copyright by AI when Regulating Online Content, or why the Answer to the Machine should (still) not be in the Machine', Paper presented at the conference "Modern Challenges of IP law" in honour of Bill Cornish, University of Warsaw, Poland, 2 September 2022 (on file with the author).

[23]We are aware that these are subject matters that present marked differences from a regulatory perspective. Our point of entry in the debate of online content moderation comes first and foremost from an IP perspective. In this context, we conceive fundamental rights as a counterweight to private ordering and to the powers of private entities as, in the creative industry in particular, large multinational corporations might try to dictate and secure a model maximising reward for themselves with little concerns for the access to works. We expand that discussion to cover—and draw conclusions for—content moderation and algorithmic enforcement at large, especially in light of the fact that the EU has traditionally set up a horizontal regulatory framework for content moderation online. For example, we do not consider the issue of disinformation in particular, which is such a broad, important current issue that would need specific treatment on its own and can only be touched upon in this piece. However, in discussing the notion of online harm and the distinction between illegal and harmful content, we consider how the legal framework might apply to disinformation as well.

mic means.[24] Operating under the Calabresi-Coase paradigm of "least-cost avoiders",[25] Online Service Providers (OSPs) are naturally inclined to minimise transaction costs associated with adjudication and liability. This predisposition may inadvertently tilt the balance toward excessive content blocking. Such a trend could culminate in a regime of imperceptible yet pervasive over-enforcement, acclimating users to a substantially sanitised digital landscape.[26] Furthermore, expansive online intermediaries' algorithmic enforcement obligations results in architectural changes leading to sanitisation of allegedly infringing content—possibly legit freedom of expression—by design. Therefore, enforcement can become implicit by modifying the architecture of the internet,[27] since, in Lessig's words, the code is the law of cyberspace.[28] The landscape of online content moderation is increasingly characterised not just by privatised governance but also by state-driven policies that—if exercised unwisely—might also veer towards suppressing freedom of expression. Such trends necessitate a reevaluation of current policies, to ensure that the balance of power between states, platforms, and users is equitably and transparently maintained, with due respect to individual liberties. In this context, the Digital Services Act (DSA) tries to reform the legal framework established by the E-Commerce Directive while avoiding over-enforcement and securing users' fundamental rights.[29] It also aims at increasing the transparency of the use of algorithmic tools for content moderation and proposes a set of regulatory oversight mechanisms for this purpose.[30] In fact, several judicial decisions have highlighted the inconsistencies between automated enforcement and fundamental rights,[31] with special emphasis on transparency and due process.[32] In this context, how are online intermediaries – gatekeepers of the internet and masters of the algorithms - supposed to balance the different interests and how can they be supervised independently to prevent that private parties decide alone on what should be online and what should not? How can regulatory intervention help avoiding a dystopian future for users, in particular in the 'black box society'?[33]

Taking fundamental rights seriously in the Digital Services Act reform, thus, becomes a high priority to avoid a dystopian future. The DSA reform apparently seeks the implementation of a more balanced regulatory framework for the digital environment where all competing fundamental rights and stakeholders' interests benefit from equal safeguards. Platform regulation is a complex conundrum in search of proportional balancing of fundamental rights and stakeholders' interests. The terms of the debate that online content moderation entails, via filtering and monitoring and the use of automated tools in particular, has been spelled out by the Court of Justice of the European Union (CJEU) multiple times.[34] According to the CJEU, when imposing obligations on internet service providers a trifecta of interests must be taken into consideration, including

[24]See, e.g., G. Frosio, 'Algorithmic Enforcement Online', in P. Torremans (ed), *Intellectual Property Law and Human Rights* (4th edition, Wolters Kluwer 2020), 709–744.

[25]See G. Calabresi, 'Some Thoughts on Risk Distribution and the Law of Torts', (1961) 70 Yale Law Journal, 499; R. Coase, 'The Problem of Social Cost', (1960) 3 *Journal of Law & Economics*, 1.

[26]But see Elkin-Koren and Husovec arguing that technologies might be the only way how we address the concerns of over-blocking on scale and with necessary speed: N. Elkin-Koren, 'Fair Use by Design' (2017) 64 UCLA L Rev 22 (2017); M. Husovec, 'The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown? Which is Superior? And Why?' (2019) 42(1) *Columbia J of Law & the Arts*, 53–84.

[27]See J. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology', (1998) 76 Texas L. Rev. 553.

[28]See L. Lessig, *The Code and Other Laws of Cyberspace* (Basic Books 1999) 3–60; W. Mitchell, *City of Bits: Space, Place, and the Infobahn* (MIT Press 1995), 111. See also L. Lessig, *Code: Version 2.0* (Basic Books 2006).

[29]See DSA, see n. 16.

[30]A few jurisdictions have already responded with new regulatory initiatives or proposals for future reform, including the Online Safety Bill or the Brazilian "Fake News" Bill. See PL (Bill) 2630/20 'Brazilian Law of Freedom, Responsibility and Transparency on the Internet' (2020) <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>. See also Proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021)0206 – C9–0146/2021–2021/0106(COD) (hereafter "AI Act Proposal") (including provisions regarding algorithmic transparency). From a data protection perspective, see, e.g., The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

[31]See in the EU, C-401/19, *Republic of Poland v European Parliament and Council of the European Union* [2022] ECLI:EU:C:2022:297 (hereafter '*Republic of Poland*')

[32]See on this issue in the context of Article 17 of the CDSM: C. Geiger and B. J. Jütte, 'Platform liability under Article 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match' (2021) 70(6) GRUR Int 517.

[33]See F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

[34]See infra, e.g., 2.2.

> the freedom of those service providers to conduct a business, guaranteed in Article 16 of the Charter, [and to respect] the fair balance between that freedom, the right to freedom of expression and information of the users of their services, enshrined in Article 11 of the Charter, and the right to intellectual property [and more broadly the private rights] of the rightsholders, protected in Article 17(2) of the Charter […].[35]

In our opinion, from a societal public interest-perspective, particular attention should be given to interests related to users' freedom of expression (and information), given the role of this fundamental right as part of 'the essential foundations of [a democratic] society, one of the basic conditions for its progress and for the development of every man.'[36] Optimal regulation in the field of platform governance must thus attempt first to preserve users' and citizens' rights, as more online enforcement – and potential over-enforcement – equates with less access to information and less freedom of expression, thus a shrinking space for debate essential to democracy. The centrality of users' rights – and the overall goal of the EU legal system to preserve those rights against invasive proactive algorithmic enforcement – has been reiterated by the Grand Chamber of the CJEU in the Case C-401/19 of 26 April 2022,[37] possibly acknowledging a fundamental right of users to share content online that cannot be limited by algorithmic content moderation.[38]

In this article, we provide further guidance for a fundamental rights approach to digital services' regulation that first and foremost must protect and enhance users' rights. In section 2, this article provides a swift overview of the present platforms' liability regime, the FRs' balancing endorsed by the ECD, including why liability exemptions have been a fundamental rights-friendly regime and should be preferred to a strict liability regime for intermediaries, and the recent developments en route to the DSA. Section 3 describes the European framework for FRs online, extracting a set of guiding principles from EU legislation and the jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR). Finally, in Section 4, this article applies the lessons learned from the legislative and judicial framework to the DSA reform, suggesting what could be considered as its optimal implementation from a FRs-centred perspective. We take in particular a regulatory approach to platform liability, based on the proposed intervention of an independent regulatory authority to ensure a fundamental rights-compliant content moderation process.

2 | PLATFORM LIABILITY REGIMES AND FUNDAMENTAL RIGHTS: FROM THE E-COMMERCE DIRECTIVE TO THE DIGITAL SERVICES ACT

Navigating the nuanced landscape of platform liability regimes and fundamental rights demands a comprehensive look at key legislative frameworks. Originating in the 1990s, early limited liability regimes aimed for a precarious

[35]C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH* [2014] EU:C:2014:192, para 52. See more detailed on the case law of the CJEU on copyright enforcement by intermediaries online, C. Geiger and E. Izyumenko, 'The Role of Human Rights in Copyright Enforcement Online: Elaborating a Legal Framework for Website Blocking', (2016) 32(1) *American University International Law Review*, 43.

[36]ECtHR, *Handyside v. United Kingdom*, Application No. 5493/72, 7 December 1976, [49]. As emphasised by the UN General Assembly, Resolution 59(1), 14 December 1946), "freedom of information is a fundamental human right and […] *the touchstone of all the freedoms* to which the United Nations is consecrated (emphasis added)"

[37]See *Republic of Poland*, see n. 31, para 80. In this context a parallel can be drawn with data protection as this case cites C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, ECLI:EU:C:2020:559, para 176. This, in turn, references Opinion 1/15, *EU-Canada PNR Agreement* [26 July 2017] EU:C:2017:592, para 140 and 141, which employs language similar to that used in the *Republic of Poland* case by noting that "the protection of the fundamental right [to respect for private life] at EU level requires, in accordance with settled case-law of the Court, that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary". See also C-817/19, *Ligue des droits humains ASBL v Conseil des ministers*,ECLI:EU:C:2022:491 (reaffirming the stance in Opinion 1/15). For a discussion of the crucial distinction between solely automated decision-making and decision-making that involves human oversight, as delineated under Article 22 of the GDPR, see a report discussing automated decision-making in courts at: https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf.

[38]See G. Frosio, 'Freedom to Share', 53 (2022) *IIC - International Review of Intellectual Property and Competition Law*, 1145–1148; J. P. Quintais and S. F. Schwemmer, 'The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?', (2022) 13(2) *European Journal of Risk Regulation*, 191, 197.

balance between user rights and the operational freedoms of DSPs. This ethos has been enshrined in the E-Commerce Directive, which stands as a landmark in shaping the responsibilities of online platforms in the European Union. However, with the advent of the Digital Single Market Strategy and the impending Digital Services Act, the policy equilibrium is being recalibrated. The new legislative thrust appears to retain some of the foundational principles while introducing more stringent obligations on platforms, thereby sparking debates about rights, responsibilities, and the overarching role of digital intermediaries in society. As the European Union seeks to harmonise and deepen its digital single market, this evolving legal framework continues to stir contentious dialogues around balancing corporate interests, user freedoms and the rule of law.

2.1 | The origins of the limited liability regime: A fundamental rights-friendly theoretical approach

With the mainstreaming of the World Wide Web in the nineties, the legislators took the decision that DSPs, both access and hosting providers,[39] should enjoy liability exemptions for unlawful acts of third parties on their networks. After initial legislation enacted in the U.S.A.,[40] the European Union—as well as multiple other jurisdictions[41]—quickly followed suit and introduced obligations on Member States to protect DSPs from liability.[42]

From a theoretical perspective, early liability exemption schemes attempt to balance the competing fundamental rights at stake.[43] In general, these schemes have been engineered under the idea that safe harbours should apply pressure to DSPs to ensure that illegal content is not being hosted on their platform under a set of caveats and limitations meant to promote public interest according to welfare theory approaches.[44] Thus, as William Fisher has explained in the context of copyright,[45] first, penalties should only be enforced upon intermediaries to prevent illegal conduct by users if the incidence of infringement would be unacceptably high, because direct infringers cannot be controlled by socially acceptable sanctions. Second, the intermediaries must be unwilling to prevent infringements on their own—and instead, might foster it. Third, the intermediaries can effectively suppress infringements with minimal capacity for direct infringers to circumvent them. Finally, intermediaries must be able to prevent infringements by third parties without a high social or economic cost. This cost–benefit analysis would be highly relevant in the case of dual-use technologies, i.e. technologies that are used to infringe others rights and also allow socially beneficial uses.[46] After being dominant in the past few decades, these intermediary liability policy approaches based on welfare cost–benefit analysis have been increasingly side-lined, as highlighted by some scholars,[47] while policy makers have been trying to push more responsibility on DSPs, often incentivising private ordering and voluntary measures.[48] This policy strategy has posed challenges from a fundamental and user rights perspective.

[39]To put it bluntly, access or mere conduit providers are telecoms that provide access to the Internet to their customers; hosting providers, instead, are applications and platforms providing web space where users can host content. See Dinwoodie, see n. 1.

[40]See Communications Decency Act of 1996, 47 U.S.C. § 230; The Digital Millennium Copyright Act of 1998, 17 U.S.C. § 512 [hereafter DMCA]

[41]See for a review of safe harbour legislation, World Intermediary Liability Map (WILMap) (a project designed and developed by G. Frosio and hosted at Stanford CIS) <https://wilmap.law.stanford.edu>.

[42]See 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 178/1–16 [hereafter ECD].

[43]See C. Geiger, G. Frosio and E. Izyumenko, 'Intermediary Liability and Fundamental Rights' in Frosio (ed), see n. 1, 138.

[44]See R. Kraakman, 'Gatekeepers: the Anatomy of a Third-Party Enforcement Strategy', (1986) 2(1) *Journal of Law, Economics and Organization*, 53.

[45]See W. Fisher, CopyrightX: Lecture 11.1, Supplements to Copyright: Secondary Liability (February 18, 2014), 7:50, <https://www.youtube.com/watch?v=7YGg-VfwK_Y> (applying Kraakman's framework to copyright infringement).

[46]D. Lichtman, 'Copyright as Information Policy: Google Book Search from a Law and Economics Perspective', in J. Lerner & S. Stern (eds), 9 *Innovation Policy and The Economy* (NBER 2008), 19 (making this welfare argument clear by applying it to YouTube).

[47]See G. Frosio and M. Husovec, see n. 14, 613–630; G. Frosio, see n. 10, 1–33; M. Husovec, see n. 14.

[48]See, e.g., European Commission Communication, see n. 14, para 3.3.2 (calling online intermediaries to adopt effective voluntary proactive measures to detect and remove illegal content online" by using automatic detection and filtering technologies); Recommendation from the Commission on Measures to Effectively Tackle Illegal Content Online, C(2018)1177final, para 37; The Strengthened Code of Practice on Disinformation 2022 < https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation> (delivered by a broad coalition of stakeholders—including major online platforms, niche and emerging platforms, advertising industry participants, fact-checkers, as well as research and civil society organisations—following the Commission's May 2021 Guidance).

2.2 | Fundamental right balancing in the E-commerce Directive liability regime

Pursuant to the mentioned public interest cost–benefit approach, the ECD also provided both access and hosting providers with exemptions to liability for illegal activities committed by users through their services. These exemptions apply horizontally to miscellaneous infringing activities. The ECD set up a limited liability regime based on two user and fundamental rights-friendly principles: (1) the principle of knowledge-and-take-down[49] and (2) the principle of no-monitoring obligation.[50] On one side, Article 14(1) of the ECD is a safe harbour that protects DSPs from liability, provided they have no knowledge of the infringement or act expeditiously to remove or disable access to the illegal content as soon as they are aware of its availability on the network. On the other side, Article 15(1) provides that for services covered by Articles 12, 13 and 14, Member States cannot impose a general obligation on Internet service providers to monitor information transmitted or stored nor a general obligation to seek facts or circumstances indicating illegal activity.[51]

The interplay of these principles serves well users' fundamental rights from multiple perspectives. First, a teleological interpretation of Articles 14 and 15 of the ECD highlights how the *ex-post* filtering set up by the present ECD's hosting exemption serves the protection of fundamental users' rights. As Van Eecke mentioned, 'the notice-and-take-down procedure is one of the essential mechanisms through which the E-Commerce Directive achieves a balance between the interests of rightsholders, DSPs and users'.[52] The ECD does create a 'negligence-based system'[53] that forces intermediaries to consider actual uses of protected works and limit overblocking and chilling effects on privileged uses, such as uses covered by exceptions and limitations, fair uses and fair dealing. By operating *ex post*, rather than *ex ante*, the ECD's hosting exemption furthers the policy goal of minimising chilling effects, especially given the critical role of virality in online content distribution.

Second, the CJEU has made clear that general proactive monitoring and filtering mechanisms are contrary to EU law.[54] First, in *Scarlet* and *Netlog* as well as *L'Oréal*, the Court precisely set the spectrum of permissible and impermissible monitoring obligations, authoritatively defining the distinction between general and specific monitoring and filtering, based on a fundamental right approach. On the one hand, in *Netlog*, referring specifically to hosting providers, the Court defines general monitoring obligations, which are prohibited. According to the CJEU, EU law must be interpreted as precluding requiring a hosting provider to install a system for filtering: (1) information which is stored on its servers by its users; (2) which applies indiscriminately to all of those users; (3) as a preventative measure; (4) exclusively at its expense; (5) for an unlimited period; and (6) which is capable of identifying electronic files containing musical, cinematographic or audio-visual works.[55] As explained in more detail in Part II, the CJEU believes that these general monitoring and filtering measures gravely limit several fundamental rights, including users' freedom of expression and privacy and DSPs' freedom to conduct a business.[56] On the other hand, *L'Oréal* makes available not only injunctions to take

[49]Reference to knowledge-and-take-down, rather than notice-and-take-down, applies more fittingly to the ECD system, which does not provide for a legislatively mandated notice-and-take-down and counter-notice procedure as in the US DMCA.

[50]See ECD, see n. 42, art 14–15.

[51]Ibid, Art 15. But see also ibid, Recital 48 (previously establishing that '[t]his Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to *apply duties of care*, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities') (emphasis added).

[52]P.Van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach', (2011) *Common Market L. Rev*., 1455, 1479–80.

[53]In tort or extra-contractual liability law, a 'negligence-based system', as opposed to a "strict-liability system', imposes liability only as a result of the failure to exercise certain duties of care. See, e.g., for further reference, V. Krapanou, 'Strict Liability Versus Negligence'. in A. Marciano and G. B. Ramello (eds), *Encyclopedia of Law and Economics* (Springer 2014).

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

[55]See *Netlog*, see n. 54, paras 26 and 52.

[56]See, in this sense, also M. Senftleben and C. Angelopoulos, 'The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market' (2020) SSRN Research Paper no 3717022 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717022> (noting that '[t]he jurisprudence of the Court of Justice of the European Union has shed light on the anchorage of the general monitoring ban in primary EU law, in particular the right to the protection of personal data, the freedom of expression and information, the freedom to conduct a business, and the free movement of goods and services in the internal market. Due to their higher rank in the norm hierarchy, these legal guarantees constitute common ground for the application of the general monitoring prohibition in secondary EU legislation').

measures that contribute to bringing to an end infringements committed through an online marketplace, but also to prevent further infringements.[57] However, according to the CJEU, an active monitoring of all the data of each of its customers in order to prevent any future infringement would be precluded by EU law.[58] Hence, the CJEU sets the boundaries of the notion of specific—and general—monitoring obligations by noting that ISPs can be only ordered to prevent further infringements (1) of that kind (2) by the same seller (3) in respect of the same trademarks.[59] In *Glawischnig-Piesczek*, the CJEU has broadened the scope of monitoring 'in a specific case' with reference to content identified as illegal by national courts as in the case of a defamatory comment posted by an anonymous Facebook user.[60] In this case, a platform like Facebook might be requested to block and remove identical content and content with equivalent meaning; however, the elements of equivalent information should be specifically identified in the injunction and the DSP should not have to carry out any independent assessment of the content.[61] However, it may remain unclear how this can be done accurately considering the current state of technology and the need to take into account context.

Third, injunctions under Article 18(1) ECD[62] should not limit freedom to conduct a business by imposing an '*excessive obligation*' on the host provider.[63] In this context, obligations cannot reach as far as disrupting platforms' business models. In *Glawischnig-Piesczek*, this is reflected in narrow specific monitoring obligations, so that the host provider should be able to identify elements of equivalent information using automated tools without carrying out an independent assessment of the content.[64] A parallel can be drawn with a long line of case law from the *Bundesgerichtshof* (BGH)—the German Supreme Court—noting that proactive monitoring obligations cannot go as far as endangering the platforms' business models.[65] In the German cases, Internet auction platforms such as eBay could not be asked to manually check all entries because that would have been economically unfeasible.[66] A further confirmation of the principle that injunctions cannot reach as far as disrupting 'normal' platforms' business models might come from the construction of the notion of passive/active hosting providers.[67] In discussing whether YouTube plays an active role leading to a loss of the liability exemption, the *Oberster Gerichtshof* (OGH)—the Austrian Supreme Court—has asked the CJEU whether Article 14 ECD should be interpreted in the sense that an online video platform plays an 'active role' when it suggests videos, facilitates search, provides help to users and shows targeted ads.[68] At the core of this case lies the question whether a platform remains neutral when it does optimise all content rather than only the infringing one. Actually, the Austrian Court of Appeal that last decided the case noted that YouTube acts and behaves according to the 'normal business model' of a host operator.[69] Structuring and search options,

[57]See C-324/09 *L'Oréal SA and Others v eBay International AG and Others* [2011] ECLI:EU:C:2011:474, para 131 (hereafter '*L'Oréal*').
[58]Ibid., para. 139.
[59]Ibid., para. 141.
[60]Case 18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Ltd*, ECLI:EU:C:2019:821 (hereafter '*Glawischnig-Piesczek*'). See also, applying the same principle to copyright protected content, *Republic of Poland*, see n. 31, para 90 (hereafter '*Republic of Poland*').
[61]ibid., paras. 35–37.
[62]This article provides that 'Member States shall ensure that court actions available under national law concerning information society services' activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved'.
[63]Ibid, para 44. See also OGH 30.03.2020, ORF/Facebook, 4Ob36 / 20b [4.1]-[4.5] (Austria) (applying *Glawischnig-Piesczek* and concluding that, for an injunction to be lawful under EU law, content similar in its core should be identifiable 'at first glance' or determined by 'technical means' which would not impose excessive control obligations on Facebook).
[64]*Glawischnig-Piesczek*, see n. 60, paras 45–46.
[65]See BGH *Rolex v Ebay/Ricardo* (a.k.a. Internetversteigerung I) [11 March 2004] I ZR 304/01, GRUR 2004, 860 (DE) para 31; BGH *Rolex v eBay* (a.k.a. Internetversteigerung II) [19 April 2007] I ZR 35/04, GRUR 2007, 708 (DE); BGH *Rolex v Ricardo* (a.k.a. Internetversteigerung III) [30 May 2008] I ZR 73/05, GRUR 2008, 702 (DE).
[66]Ibid.
[67]See ECD, see n. 42, Recital 42 (providing that exemptions apply only to passive providers, when 'the activity of the information society service provider [...] is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored').
[68]See Case 500/19 *Puls 4 TV GmbH & Co. KG v YouTube LLC and Google Austria GmbH*, Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 1 July 2019. See also R. Schultes, 'Puls 4 v YouTube in Austria does not anticipate Article 17', *Kluwer Copyright Blog*, 2 April 2019, <http://copyrightblog.kluweriplaw.com/2019/04/02/puls-4-v-youtube-in-austria-does-not-anticipate-article-17>.
[69]See Handelsgericht Wien [Higher Regional Court of Vienna] *Puls 4 TV GmbH & Co. KG v YouTube LLC and Google Austria GmbH* [13 February 2019] case no 4 R 119/18a, 10 [hereafter *Puls 4 v YouTube*]

therefore, are standard user friendly-features, which are applied to all content indiscriminately and automatically all over the platform.[70] Foregoing them in order not to lose neutrality would amount, according to the Austrian Court, to losing all user-friendliness.[71] Therefore, one might argue, expanding the notion of active provider to features dictated by common standards of user friendliness would amount to jeopardising the platform's business model and curtailing its freedom to conduct business.

At the same time, the liability exemption regime is not absolute; instead, it is engineered via the inclusion of a number of rightholder-friendly exceptions to the general liability regime. First and foremost, notwithstanding the applicability of the exemptions, injured parties can always seek injunctions against a DSP to stop the effects of an ongoing infringement or prevent further infringements.[72] Second, the ECD liability regime provides that exemptions apply only to passive providers, when 'the activity of the information society service provider [...] is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored'.[73] The CJEU has clarified that Article 14 applies to ISPs who do not play 'an active role of such a kind as to give it knowledge of, or control over, the data stored'.[74] In contrast, when the operator of a platform like eBay 'has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role'.[75] The extent of the notions of passivity and activity, optimisation and promotion have been long debated, wondering whether *inter alia* user-generated content platform, such as Facebook or YouTube, would be passive or active, as it was discussed by the case law of the Austrian Supreme Court mentioned above.[76] Third, as already mentioned above, the ECD makes uncompliant with EU law general monitoring obligations only, meaning that, first, monitoring and filtering technologies set up by an intermediary on a voluntary basis, such as YouTube' Content ID, are lawful under EU law as well as, second, specific monitoring obligations as defined by the CJEU in *L'Oréal* and *Glawischnig-Piesczek* case law mentioned earlier. Finally, tightly connected with the potential imposition of specific monitoring and filtering obligations and the availability of injunctions to prevent infringement, Recital 48 of the ECD specifically provides that Member States can 'requir[e] service providers, who host information provided by recipients of their service, to apply *duties of care*, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities'.[77]

2.3 | Respecting fundamental rights in the DSM: from the C-DSM Directive to the DSA

This balanced, fundamental right-friendly limited liability regime established by the ECD has been under discussion for some time as part of the debate surrounding the implementation of the Digital Single Market Strategy (DSMS). In

[70]ibid., 11.

[71]ibid.

[72]See, e.g., Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, 2001 O.J. (L 167) 10–19 [hereafter InfoSoc Directive] art 8(3); Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2000 on the Enforcement of Intellectual Property Rights, 2004 O.J. (L 195) 16 [hereafter Enforcement Directive], art 11.

[73]ECD, see n. 42, Recital 42.

[74]Cases 236/08 to 238/08 *Google France SARL and Google Inc. v Louis Vuitton Malletier SA, Google France SARL v Viaticum SA and Luteciel SARL and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others*, ECLI:EU:C:2010:159, para 120.

[75]*L'Oréal*, see n. 57, para. 116.

[76]See *Puls 4 v YouTube*, see n. 69. Cf. G. Sartor, 'Providers Liability: From the eCommerce Directive to the future' In-Depth Analysis for the IMCO Committee [2017] IP/A/IMCO/2017–07, 26 (noting that 'we must abandon the view that only "passive" intermediaries should be protected i.e., the view that intermediaries that take a "non-passive", or "active role"—by indexing user-generated content, or linking advertising to it, or determining what results will be provided to user queries—should lose their protection from secondary liability. What justifies the exemption from secondary liability is not the passivity of intermediaries, but rather their function as communication enablers. This function would be incompatible with initiating the communications at issue, but may allow or even require playing an active role in creating an environment in which users' communications can be delivered and made accessible'.)

[77]See ECD, see n. 42, Recital 48.

order to move 'towards a connected digital single market',[78] the EU Commission planned to clarify the rules applicable to DSPs in relation to distribution of copyright protected works, while considering '[m]easures to safeguard fair remuneration of creators [...] in order to encourage the future generation of content'.[79] To this end, the DSMS sought to introduce enhanced obligations on platforms and other Internet intermediaries when dealing with infringing third parties.[80] A heated debate has emerged about the regulations that apply to a subset of intermediaries called 'online platforms' and 'whether to require intermediaries to exercise greater responsibility and due diligence in the way they manage their networks and systems—a duty of care'.[81]

As a result of multiple consultations, the Commission apparently chose to maintain the existing intermediary liability regime in their *Communication on Online Platforms and the Digital Single Market*.[82] However, the Commission also emphasised that 'a number of specific issues relating to illegal and harmful content and activities online have been identified that need to be addressed'.[83] This would result in the introduction of a 'sectorial legislation [...] and problem-driven approach'.[84] In order to achieve this, a number of legislative interventions have been taken—or might be in the future—including revising current copyright regulations and the endorsement of voluntary self-regulatory actions.[85] As part of a broader move to modernise the EU copyright regulations in the DSM,[86] the Commission looked to promote a fairer allocation of value from the distribution of copyrighted material online with some targeted provisions in the C-DSM Directive.[87] In shaping Online Content Sharing Service Providers' (OCSSPs) liability,[88] the new legislation brought about widespread concerns regarding fair balancing of the new provisions with fundamental rights of users[89] to the extent that Poland challenged the new OCSSPs' obligations before the CJEU on this very basis, with the CJEU rejecting the request of annulment but making important clarifications to preserve users' rights.[90]

Shortly after the approval of the C-DSM Directive, the European Commission (EC) announced a DSA package. One of the two aims of the DSA is 'to deepen the Single Market for Digital Services, by increasing and harmonising

[78]See European Commission Communication, 'A Digital Single Market Strategy for Europe' COM (2015) 192 final, para 3.3

[79]Ibid., para 2.4.

[80]Ibid., para 3.3.2.

[81]ibid. See also ECD, see n. 42, Recital 48.

[82]See European Commission Communication, 'Online Platforms and the Digital Single Market: Opportunities and Challenges for Europe' COM (2016) 288 Final, 9.

[83]Ibid., 8.

[84]Ibid.

[85]ibid. Another intervention worth mentioning is the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, 2022/0155(COD), which serves as a specialised legal framework for protecting children in the digital age, and thus holds particular relevance.

[86]See European Commission, Digital Single Market, Modernisation of the EU Copyright Rules <http://bit.ly/DSMCopyright16>.

[87]See Directive 2019/790/EU, see n. 11, Article 17 (providing that a subset of online platforms, known as Online Content Sharing Service Providers, are now directly liable for communicating to the public copyright infringing content that their users might make available on their networks, thus, under certain conditions, OCSSP have an obligation either to (1) conclude licencing agreements to make available that protected content on the platforms or (2) make 'best efforts' to make unavailable any infringing content on their networks, which might turn *de facto* in an obligation to set up proactive monitoring and filtering or so-called 'upload filters'). See also Giancarlo Frosio, 'Reforming the C-DSM Reform: a User-Based Copyright Theory for Commonplace Creativity' (2020) 52(6) IIC 709–750.

[88]Ibid., art 2(6) (defining the notion of OCSSPs that *de facto* matches closely that of UGC platforms).

[89]For a comprehensive analysis see C. Geiger and B. J. Jütte, see n. 32,517.

[90]See *Republic of Poland*, see n. 31. See also, for a commentary of the clarifications provided by the CJEU, Frosio, see n. 38; C. Geiger and B.J. Jütte, 'Constitutional Safeguards in the "Freedom of Expression Triangle"—Online Content Moderation and User Rights after the CJEU's Judgement on Article 17 Copyright DSM Directive' (*The Digital Constitutionalist*, 31 May 2022) <https://digi-con.org/constitutional-safeguards-in-the-freedom-of-expression-triangle> (also available on *Kluwer Copyright Blog*, 6 June 2022). On this action for annulment and on the inherent contradictions of Art. 17 C-DSM Directive that surfaced on the occasion of the first hearing held by the CJEU, see P. 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*, 11 November 2020); J. Reda, J. Sellinger and M. Servatius, 'Article 17 of the Directive on Copyright in the Digital Single Market: a Fundamental Rights Assessment' (2020) Study for the Gesellschaft für Freiheitsrechte <https://freiheitsrechte.org/home/wp-content/uploads/2020/11/GFF_Article17_Fundamental_Rights.pdf>. See also Geiger and Jütte, see n. 89 (arguing that Article 17 is incompatible with the constitutional framework of the EU and this should lead to the annulment of at least certain portions of the provision, and if not, possibly, the provision in its entirety); M. Husovec, 'Over-Blocking: When is the EU Legislator Responsible?' (2020) SSRN Research Paper no. 3784149 <https://papers.ssrn.com/ abstract_id = 3,784,149 > (concluding that the CJEU should invalidate Article 17 because it lacks any effective ex-ante safeguards and the ex-post safeguards are insufficiently specific, irrespective of whether Member States can redress this limitations at the implementation stage); M. Cloutier, 'Poland's Challenge to EU Directive 2019/790: Standing up to the Destruction of European Freedom of Expression' (2020) 125 *Dickinson Law Review*, 161, 161–197.

the responsibilities of online platforms and information service providers and reinforce the oversight over platforms' content policies in the EU'.[91] As pointed out by the Commission, the basic principles characterising the ECD should be kept in place: '[t]he European Single Market requires a modern legal framework to ensure the safety of users online and to allow innovative digital businesses to grow, while respecting the basic principles underpinning the current legal framework of the e-Commerce Directive'.[92] In preparation of the DSA, on 19 October 2020, the European Parliament (EP) adopted three resolutions, namely on: (1) the fundamental rights issues posed by the DSA (EP Resolution on the DSA and FRs)[93]; (2) improving the functioning of the Single Market (EP Resolution on the DSA and the Single Market)[94]; and (3) adapting commercial and civil law rules for commercial entities operating online (EP Resolution on the DSA and commercial and civil rules).[95] In its resolutions, the EP aimed to keep fundamental rights at the heart of the DSA, seeking to both 'strengthen the internal market freedoms and guarantee the fundamental rights and principles set out in the Charter'.[96] Since the modernisation of the e-commerce rules can affect fundamental rights, the Commission had an imperative to be 'extremely vigilant in its approach and [...] integrate international human rights standards into its revision'.[97]

In this regard, to craft a balanced regulatory framework, fundamental rights protection needed to serve as an overarching principle of the EU digital services policy, necessitating the incorporation of more robust and explicit fundamental rights language.[98] In particular, the DSA needed to comply with Article 52(1) EU Charter that imposes an obligation to respect the essence of rights and freedoms and introduces the principle of proportionality. The EU legislature had the responsibility to ensure first, and prior to Member States and the CJEU,[99] a proper balance of fundamental rights in the DSA, explicitly tying the obligations of DSPs to these rights. Given that both Member States and DSPs have a duty to respect fundamental rights and comply with all applicable laws,[100] articulating this relationship in terms of fundamental rights would ensure that in case of disputes on the exact scope of DSPs' obligations the link to fundamental rights is evident. Such clarity would serve as a guide, particularly for courts, in interpreting DSPs' obligations in a manner consistent with legislative intent and, consequently, in accordance with fundamental rights.

The DSA tries to achieve these goals, first, with some general reference to the underlying fundamental rights framework. Of course, the resolution on the 'Digital Services Act and fundamental rights issued posed' had already highlighted from the inception the central role of fundamental rights in online regulation, and for the DSA in particular.[101] Specific reference to the key role of fundamental rights' protection in digital services' regulation abounds in the DSA, starting from the Explanatory Memorandum, which ensures safeguards for fundamental rights and reminds that the ECD prohibition of general monitoring obligation is crucial to the fair balance of fundamental rights in the online world. According to the Explanatory Memorandum, general monitoring obligations 'could disproportionately

[91]A. De Streel et al., *Online Platforms' Moderation of Illegal Content Online: Law, Practices and Options for Reform*, Study for the committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020, <https://europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf>.

[92]See The Digital Services Act package <https://ec.europa.eu/digital-single-market/en/digital-services-act-package>.

[93]European Parliament, 'Resolution on the Digital Services Act and fundamental rights issues posed' [2020/2022(INI)] 20 October 2020, Provisional edition, P9_TA-PROV(2020)0274 <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0274_EN.html> (hereafter 'EP Resolution on the DSA and FRs').

[94]European Parliament, Resolution on the Digital Services Act: Improving the functioning of the Single Market [2020/2018(INL)] 20 October 2020, Provisional edition, P9_TA-PROV(2020)0272, <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html> (hereafter 'EP Resolution on the DSA and the Single Market').

[95]European Parliament, Resolution on the Digital Services Act: adapting commercial and civil law rules for commercial entities operating online [2020/2019 (INL)] 20 October 2020, Provisional edition, P9_TA-PROV(2020)0273, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0273_EN.html (hereafter 'EP Resolution on the DSA and commercial and civil rules').

[96]EP Resolution on the DSA and the Single Market, see n. 94, point 22.

[97]EP Resolution on the DSA and FRs, see n. 93, point 19.

[98]ibid.

[99]Cf. Case 275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, ECLI:EU:C:2007:454, Opinion of AG Kokott, para 56 (noting that MS transposals and CJEU's interpretation can only follow up on initial balancing from the EU legislator).

[100]Cf. D. Leczykiewicz, 'Horizontal Effect of Fundamental Rights: In Search of Social Justice or Private Autonomy in EU Law?' in U. Bernitz, X. Groussot, F. Schulyok (eds), *General Principles of EU Law and European Private Law* (Kluwer Law International, 2013), 171–186 (noting that the EU Charter has been extended to horizontal situations involving two private parties).

[101]See EP Resolution on the DSA and FRs, see n. 93.

limit users' freedom of expression and freedom to receive information, and could burden service providers excessively and thus unduly interfere with their freedom to conduct a business'.[102] Again, Recital 3 of the DSA stresses that a responsible behaviour of DSPs is essential for allowing the exercise of the fundamental rights guaranteed in the EU Charter, 'in particular the freedom of expression and information and the freedom to conduct a business, and the right to non-discrimination'.[103] Finally, the DSA should be interpreted and applied in accordance to the fundamental rights recognised by the EU Charter with an obligations for public authorities exercising the powers provided by the DSA to achieve a fair balance of the conflicting fundamental rights, in accordance with the principle of proportionality.[104]

However, the DSA also includes some specific prescriptive obligations for DSPs to enforce fundamental rights. First, by defining its scope, the DSA states that the aim of the Regulation is to regulate an online environment 'where fundamental rights enshrined in the Charter are *effectively* protected'.[105] Second, the DSA has included the impact of digital services on the exercise of fundamental rights protected by the EU Charter as a category of systemic risks that should be assessed in depth by very large online platforms (VLOPs) and very large online search engines (VLOSEs),[106] a new category of online platform to which special obligations apply.[107] VLOPs and VLOSEs must also take mitigating measures as a result of the systemic risk assessment they carry out in connection to the functioning of their services. In particular, the risk assessment of platforms' services must regard the impact of digital services on (i) human dignity (ii) the freedom of expression and information, (iii) personal data, (iv) the right to private life, (v) the right to non-discrimination and (vi) the rights of the child and (vii) consumer protection.[108] Finally, the DSA highlights the role of fundamental rights in conjunction with the emerging sensitive issues of the extra-territorial enforcement of DSPs' obligations, which has been recently debated before the CJEU and other international courts.[109] Fundamental rights must be taken into consideration among the conditions to define the territorial scope of 'orders to act against illegal content', which should 'not exceed what is strictly necessary to achieve its objective'.[110] On one side, the territorial—and extraterritorial scope—will be determined by EU and national law but also by the proportional balancing of fundamental rights that emerges from the EU Charter. On the other side, the territorial scope should be, however, limited by international law principles, including comity, according to what the CJEU established in *CNIL* and *Glawischnig-Piesczek*.[111]

Through the DSA, the European Parliament appears to be advancing a process of constitutionalisation of Internet governance. This represents a significant shift from an emphasis on private ordering solutions rooted in a liberal economic framework to a more democratic approach grounded in the protection of fundamental rights. Efforts to draft an "Internet Bill of Rights" date back to the mid-1990s,[112] and over the past three decades, these aspirational principles have increasingly begun to crystallise into law. Numerous global initiatives now fall under the rubric of

[102]See Proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 (hereafter "DSA Proposal"), 12.
[103]DSA, see n. 16, Recital 3.
[104]Ibid., Recital 153.
[105]Ibid., Article 1(1) (emphasis added).
[106]Ibid., Recital 79–86, Article 34(1)(b).
[107]Ibid., Recital 79, Article 33 (including "online platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million").
[108]ibid., Article 34.
[109]See also, for a detailed overview of the issue of extra-territorial enforcement of intermediary liability obligations and fundamental rights related tensions, G. Frosio, 'Enforcement of European Rights on a Global Scale' in Eleonora Rosati (ed), *Routledge Handbook of European Copyright Law* (Routledge 2021), 414–440. See also more generally, proposing alternative approaches regarding enforcement of copyright in the online world, C. Geiger, 'Challenges for the Enforcement of Copyright in the Online World: Time for a New Approach' in P. Torremans (ed), *Research Handbook on the Cross-Border Enforcement of Intellectual Property* (Edward Elgar 2014), 704.
[110]DSA, see n. 16 Recital 36.
[111]See Case 507/17 *Google LLC v Commission nationale de l'"informatique et des libertés* (CNIL), ECLI:EU:C:2019:772, para 64–72; *Glawischnig-Piesczek*, see n. 60, para 48–52.
[112]See L. Gill, D. Redeker, and U. Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights' (2015) Berkman Center Research Publication no. 2015–15 <https://dash.harvard.edu/handle/1/28552582>.

'digital constitutionalism'.[113] While these initiatives vary widely—in scope, origin, and form, from advocacy statements to intergovernmental positions, from judicial interventions to drafted legislation—they collectively contribute to an emergent proto-constitutional discourse. This discourse aims to establish a cohesive framework of rights, principles, and governance norms for the digital realm but also participate to the emergence of new governance structures and regulatory bodies to efficiently protect fundamental rights in a fast-moving technological environment. The DSA represents a significant milestone in the evolving landscape of digital constitutionalism. However, this trend is not confined to the European Union; it is manifesting globally across multiple jurisdictions. Recent legislative initiatives, such as the UK's Online Safety Bill and Brazil's "Fake News" Bill,[114] also signify a shift toward legitimising online speech moderation through public governance. This multilayered approach to digital constitutionalism appears to be emerging as a viable solution to the current legitimacy crisis surrounding privately managed online content moderation.

Building upon the DSA's explicit emphasis on fundamental rights—ranging from freedom of expression to freedom to conduct a business, and from the right to an effective remedy to privacy and data protection—we now turn our focus to the overarching EU framework for fundamental rights online. Ensuring a balanced approach to these competing rights, especially freedom of expression, continues to be a significant and delicate task in the ongoing DSA reform and more broadly in the platform society.[115]

3 | THE EU FRAMEWORK FOR FUNDAMENTAL RIGHTS ONLINE: EXTRACTING GUIDING PRINCIPLES FOR THE PLATFORM LIABILITY REGIME

In order to guarantee proportional balancing of fundamental rights in the DSA, reference must be primarily made to the legal framework set up both by the Charter of Fundamental Rights of the European Union (EU Charter) and the European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention of Human Rights or ECHR),[116] as construed respectively by the CJEU and the ECtHR. Only the strict application of the fundamental rights that can be extracted from this legal framework which binds Member States' obligations can help

[113]On this theory, see E. Celeste, *Digital Constitutionalism, The Role of an Internet Bill of Rights* (Routledge 2023); G. De Gregorio, 'Digital Constitutionalism in Europe, Reframing Rights and Powers in the Algorithmic Society' (CUP 2022); O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet, A Road towards Digital Constitutionalism?* (Bloomsbury 2021); E. Celeste, 'Digital constitutionalism: a new systematic theorisation' (2019) 33 *International Review of Law, Computers & Technology*, 76–99; Gill, Redeker, and Gasser, see n. 112. For a brief discussion in the context of the DSA, see G. Frosio, 'Platform Responsibility in the Digital Services Act: Constitutionalising, Regulating, and Governing Private Ordering' in A. Savin and J. Trzaskowski (eds), *Research Handbook on EU Internet Law* (Edward Elgar, forthcoming 2023). In the IP context, see C. Geiger and B. J. Jütte, 'Digital Constitutionalism and Copyright Reform: Securing Access to through Fundamental Rights in the Online World' (*The Digital Constitutionalist*, 24 January 2022) <http://digi-con.org/digital-constitutionalism-and-copyright-reform-securing-access-through-fundamentalrights-in-the-online-world>; 'Designing Digital Constitutionalism: Copyright Exceptions and Limitations as a Regulatory Framework for Media Freedom and the Right to Information Online' in M. Senftleben et al. (eds), Cambridge Handbook of Media Law and Policy in Europe (CUP, forthcoming 2024), preprint available at <https://ssrn.com/abstract=4548510>.

[114]See Online Safety HC Bill (2022–2023) <https://bills.parliament.uk/bills/3137> (awaiting Royal Assent); PL (Bill) 2630/20 'Brazilian Law of Freedom, Responsibility and Transparency on the Internet' (2020) < https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>.

[115]Valentina Moscon, 'Free Circulation of Information and Online Intermediaries – Replacing One "Value Gap" with Another' (2020) IIC Vol. 61, 977, <https://link.springer.com/article/10.1007/s40319-020-00982-3>.

[116]See Charter of Fundamental Rights of the European Union, 2012 OJ (C 326) 391 (hereafter 'EU Charter'); Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (hereafter 'ECHR'). The ECHR binds the EU legislator as a general principle of EU (see Art. 6(3) TEU: "Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law"). It is moreover an influential human rights framework that predates the EU Charter. All EU Member States are signatories to the ECHR, making its interpretation important to EU human rights standards. Article 6(2) of the EU Treaty mandates EU accession to the ECHR, a process that is currently under negotiation. See, e.g., Council of Europe and the European Commission, 'The EU's accession to the European Convention on Human Rights: Joint statement on behalf of the Council of Europe and the European Commission', 29 September 2020, <https://www.coe.int/en/web/portal/-/the-eu-s-accession-to-the-european-convention-on-human-rights?fbclid=IwAR1WA2amUsCVx0zAImKRzEcmWpNbvhtDU20tObfsXOmBCX4o0jldxfvDO3c>. Per Articles 52(3) and 53 of the EU Charter, any rights overlapping with the ECHR should align in scope and meaning, although EU law can offer broader protections. Given this relationship, the ECHR and ECtHR case-law are vital for shaping a balanced approach to online rights enforcement within the EU:

secure a coherent legislative framework and a horizontal, fundamental-rights compliant approach in the different legislative interventions.[117]

The liability of DSPs has implications for several fundamental rights which makes their regulation rather complex. On the one hand, DSPs' content moderation choices, increasingly through the use of algorithms, have a significant impact on users' fundamental rights, including freedom of expression, freedom of information, and the right to privacy and data protection. On the other hand, DSPs deal with preventing the online infringement of IP rights, which are protected, as a special type of property, by Article 17(2) of EU Charter.[118] Further, if there are overly strict or expansive obligations placed on DSPs, it could be in conflict with their freedom to conduct business. In particular, in order to enforce IP and other rights, some DSPs are using algorithms to make decisions which can potentially affect a cross-section of society. Despite some of these uses of algorithms having a substantial impact on many people, there is generally very little understanding of these processes[119] and of their potential tension with the ECHR and the EU Charter.[120] In this section, we seek to shed some light on the complicated effects of intermediary liability on the competing rights of users, DSPs and other stakeholders, providing a roadmap for a fair balancing within the DSA framework.

3.1 | Scope and normative content of the fundamental rights of users

The laws and regulations governing DSPs hold sweeping consequences not only for platforms themselves but, crucially, for the user's most cherished liberties. In this intricate legal landscape, the rights of users take centre stage, emerging as the linchpin around which key discussions revolve. From our ability to speak freely and access information to our expectations of privacy and due process, the policies that guide DSPs touch upon the core principles that underlie a democratic society. As we delve into these issues, we'll explore the nuances of how these fundamental rights intersect and occasionally conflict, particularly in an era of evolving obligations for online platforms. The challenge is not just to understand these rights in isolation but to negotiate the fine balance among them in a world ever more mediated by technology.

[117]Cf, in this very sense, 'Commission renews its commitment to strengthen fundamental rights in the EU', Press release, 2 December 2020 <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2249> (where the Commission announces a new Strategy to strengthen the application of the Charter of Fundamental Rights in the EU, including stronger controls regarding how/whether new legislation respects EU fundamental rights); specifically, on the horizontal effect of the fundamental rights, see T. Wischmeyer and P. Meißner, 'Horizontalwirkung der Unionsgrundrechte – Folgen für den Digital Services Act' (2023) 76(37) *Neue Juristische Wochenschrift* 2673–2678; on the evolution of the DSA in light of the CJEU's case law, see, F. Wilman, 'Between preservation and clarification: The evolution of the DSA's liability rules in light of the CJEU's case law' (*Verfassungsblog*, 2 November 2022) <https://verfassungsblog.de/dsa-preservation-clarification>.

[118]For further discussion, see C. Geiger, 'Intellectual Property Shall be Protected!? Article 17(2) of the Charter of Fundamental Rights of the European Union: A Mysterious Provision with an Unclear Scope', (2009) 31(3) *European Intellectual Property Review*, 113; C. Geiger, 'Intellectual 'Property' After the Treaty of Lisbon, Towards a Different Approach in the New European Legal Order?' (2010) 32(6) *European Intellectual Property Review*, 255; J. Griffiths and L. McDonagh, 'Fundamental Rights and European IP Law – The Case of Art 17(2) of the EU Charter' in C. Geiger (ed), *Constructing European Intellectual Property: Achievements and New Perspectives* (Edward Elgar 2013), 75; and M. Husovec, 'The Essence of Intellectual Property Rights Under Article 17(2) of the EU Charter' (2019) 20 *German Law Journal*, 840; M. Ricolfi, 'Commento all'Art. 17 – La Protezione della Proprietà Intellettuale' in Mastroianni and others (eds), *Carta dei Diritti Fondamentali dell'Unione Europea* (Giuffrè Editore 2017),

[119]This very much recalls a previous lively discussion that emerged in the context of the 2001 Copyright Directive regarding technical protection measures (TPM) protected by that legislation sometimes at the expenses of limitations and exceptions foreseen by the same Directive. See on the issue, C. Geiger, 'The Answer to the Machine should not be the Machine, Safeguarding the Private Copy Exception in the Digital Environment', (2008) 30 *European Intellectual Property Review*, 121.

[120]See *Akdeniz v Turkey* App. no. 20877/10 (ECtHR, 11 March 2014); *UPC Telekabel*, see n. 35; *Netlog*, see n. 54, paras 36–8. See also C. Geiger and E. Izyumenko, 'Blocking Orders: Assessing Tensions with Human Rights' in Frosio (ed), see n. 1, 566; C. Geiger and E. Izyumenko, 'The Role of Human Rights in Copyright Enforcement Online: Elaborating a Legal Framework for Website Blocking', (2016) 32(1) *AUILR*, 43; J. Barata and M. Bassini, 'Freedom of Expression in the Internet: Main Trends of the Case Law of the European Court of Human Rights' in O. Pollicino and G. Romeo (eds), *The Internet and Constitutional Law: The Protection of Fundamental Rights and Constitutional Adjudication in Europe* (Routledge 2016); S. Kulk and F. Zuiderveen Borgesius, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases', (2012) 34 *European Intellectual Property Review*, 791, 791–4; E. Psychogiopoulou, 'Copyright enforcement, human rights protection and the responsibilities of internet service providers after Scarlet', (2012) 34 *European Intellectual Property Review*, 552, 555; Geiger and Jütte, see n. 89.

3.1.1 | Freedom of expression, freedom to receive information and internet access

First and foremost, the regulation of DSPs, especially through imposing obligations that alter how users interact with digital services, is likely to have a significant impact on users' fundamental rights to freedom of information and expression. The fundamental right to freedom of expression, under Article 11 EU Charter and Article 10 ECHR, is sometime considered as the 'European First Amendment'.[121] This right does not solely guarantee the right to impart information but also the right of the public to receive information,[122] including the 'right to internet access', a right that is becoming fundamental in the eyes of many.[123] The rationale behind the 'right to internet access' is that 'the Internet, by facilitating the spreading of knowledge, increases freedom of expression and the value of citizenship'.[124] The French Constitutional Council expressed in a June 2009 decision on the first graduated response—HADOPI—law that '[i]n the current state of the means of communication and given the generalized development of public online communication services and the importance of the latter for the participation in democracy and the expression of ideas and opinions, [the right to freedom of expression] implies freedom to access such services'.[125] The fundamentality of the right of access to the Internet has also been highlighted by several high-profile organisations, including the UN Human Rights Council[126] and the ITU-UNESCO Commission.[127] Further, the Costa Rican Constitutional Court ruled that access to Internet is essential to the application of other fundamental rights[128] and the Finnish government officially made broadband a legal right.[129]

The Council of Europe (CoE) expressly stated that access to the Internet is a 'fundamental right' during a response to a proposal on three strike legislation.[130] The ECtHR conducted a survey of legislation in twenty Council of Europe Member States:

> The right to Internet access is considered to be inherent in the right to access information and communication protected by national Constitutions and encompasses the right for each individual to participate in the information society and the obligation for States to guarantee access to the Internet for their citizens.[131]

[121]D. Voorhoof, 'Het Europese "First Amendment": de vrijheid van expressie en informatie en de rechtspraak van het EHRM betreffende art 10 EVRM (1994–1995)' (1995) *Mediaforum* (Amsterdam), 11. See also D. Voorhoof, 'Freedom of expression and the right to information: Implications for copyright' in in C. Geiger (ed), *Research Handbook on Human Rights and Intellectual Property* (Edward Elgar 2015), 331; C. Geiger, *Droit d'auteur et droit du public à l'information, Approche de droit comparé* (Paris Litec 2004), 166.

[122]See eg *Times Newspapers Ltd (Nos 1 and 2) v United Kingdom* App. nos 3002/03 and 23,676/03 (ECtHR, 10 March 2009) para 27; *Ahmet Yildirim v Turkey* App. no. 3111/10 (ECtHR, 18 December 2012) (hereafter '*Yildirim*') para 50; *Guseva v Bulgaria* App. no. 6987/07 (ECtHR, 17 February 2015) para 36; *Cengiz and Others v Turkey* App. nos 48,226/10 and 14,027/11 (ECtHR, 1 December 2015) (hereafter '*Cengiz*') para 56. On the public's right to receive information, see also C, Geiger, 'Author's Right, Copyright and the Public's Right to Information: A Complex Relationship', in Fiona Macmillan (ed.), *New Directions in Copyright Law* (Edward Elgar 2007), Vol. 5, 24.

[123]See on this question, N. Lucchi, 'Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression', (2011) 19(3) Cardozo Journal of International and Comparative Law 645; M. Land, 'Toward an International Law of the Internet', (2013) 54(2) Harvard International Law Journal 393.

[124]See M. Conley and C. Patterson, 'Communication, Human Rights and Cyberspace', in Steven Hick, Edward Halpin, and Eric Hoskins (eds), *Human Rights and the Internet* (Macmillan 2000), 211.

[125]Conseil constitutionnel [Constitutional Council], Decision no. 2009–580 DC of 10 June 2009, s. 12. See, on this decision and its impact on copyright enforcement online, C. Geiger, 'Challenges for the Enforcement of Copyright in the Online World: Time for a New Approach', in P. Torremans (ed), *Research Handbook on the Cross-Border Enforcement of Intellectual Property* (Edward Elgar 2014), 704.

[126]See UN General Assembly, Human Rights Council Resolution, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' A/HRC/RES/20/8, twentieth session, 16 July 2012.

[127]See K. Mara, 'ITU-UNESCO Broadband Commission Aims at Global Internet Access' (*IPWatch*, 10 May 2010).

[128]See Acceso a Internet es un derecho fundamental' (*Nacion*, 8 September 2010) <http://www.nacion.com/2010-09-08/ElPais/NotasSecundarias/ElPais2514038.aspx>.

[129]See 'Finland Makes Broadband a Legal Right' (*BBC News*, 1 July 2010) <http://www.bbc.co.uk/news/ 10,461,048 > .

[130]See Monika Ermert, 'Council of Europe: Access to Internet is a Fundamental Right' (*IPWatch*, 8 June 2009); 'Internet Access is a Fundamental Right' (*BBC News*, 8 March 2010) http://news.bbc.co.uk/2/hi/technology/8548190.stm.

[131]*Yildirim*, see n. 122, para. 31.

This seems to make any action that affects the accessibility of the Internet an interference with the rights guaranteed by Article 10 ECHR.[132] In particular, websites, as means of dissemination of information, benefit from the protection afforded under Article 10 ECHR, since 'any restriction imposed on such means necessarily interferes with the right to receive and impart information'.[133] Consequently, a Google service to facilitate the creation and sharing of websites[134] as well as a video-hosting website[135] and a website which enabled users to share digital content[136] were regarded as means of dissemination of information. Article 11 EU Charter, combined with the interpretative framework of Article 10 ECHR, provides at least five conditions that can be extracted from the practice of the European Courts and that a court must consider when ruling on a website-blocking case. First, the manner of the site usage, second, the effect on legitimate communication caused by blocking the site, third, the public interest in accessing the information, fourth, if the information is available in another form, and fifth, the effect on Internet users and intermediaries under Article 10 ECHR.[137] The European Commission echoed this by stating:

> Any limitations to access to the Open Internet can impact on end-user's freedom of expression and the way in which they can receive and impart information. Although operators need to manage Internet traffic in order to ensure the proper functioning of the networks (including managing network congestion, security threats, etc.), there are many instances when unjustified blocking and throttling occurs.[138]

In the cases of *Vladimir Kharitonov v. Russia*,[139] *OOO Flavus and Others v. Russia*,[140] *Bulgakov v. Russia*,[141] and *Engels v. Russia*,[142] the ECtHR addressed the problem of wholesale blocking. Where the authorities targeted entire websites without distinguishing between legal and illegal content, it was found to be the equivalent of banning a newspaper or television station.[143] This 'deliberately disregards the distinction between the legal and illegal information the website may contain, and renders inaccessible large amounts of content which has not been identified as illegal'.[144] The ECtHR examined blocking measures where whole websites were blocked due to a single piece of content as well as continued blocking even after infringing content had been removed.[145] All these measures were found to be unlawful, including in cases regarding prohibited e-books[146] and information about filter-bypassing technologies.[147]

[132]See *Cengiz*, see n. 122, para. 57.
[133]*Yildirim*, see n. 122, para 50. See also *Cengiz*, see n. 122, para 56.
[134]See *Yildirim*, see n. 122, para. 49.
[135]See *Cengiz*, see n. 122, para. 54.
[136]See *Neij and Sunde Kolmisoppi v Sweden* (dec.) App. no. 40397/12 (ECtHR, 19 February 2013).
[137]See, for further detailed discussion, Geiger and Izyumenko, 'Blocking Orders', see n. 120, 566; Geiger and Izyumenko, 'The Role of Human Rights in Copyright Enforcement Online', see n. 120). C. Geiger and E. Izyumenko, 'Intellectual Property before the European Court of Human Rights' in C. Geiger, C.A. Nard and X. Seuba (eds), *Intellectual Property and the Judiciary* (EIPIN series Vol. 4, Edward Elgar 2018), 9.
[138]European Commission, 'Staff Working Document, Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No. 1211/2009 and (EU) No. 531/2012' SWD (2013) 331 final, s. 3.4.
[139]App. no. 10795/14 (ECtHR, 23 June 2020) (hereafter '*Kharitonov*'). For commentary, see E. Izyumenko, 'European Court of Human Rights Rules That Collateral Website Blocking Violates Freedom of Expression', (2020) 15(10) JIPLP 774.
[140]App. nos 12,468/15, 23,489/15 and 19,074/16 (ECtHR, 23 June 2020) (hereafter '*Flavus*').
[141]App. no. 20159/15 (ECtHR, 23 June 2020) (hereafter '*Bulgakov*').
[142]App. no. 61919/16 (ECtHR, 23 June 2020) (hereafter '*Engels*').
[143]*Kharitonov*, see n. 139, para 38; *Flavus*, see n. 140, para 37. One might juxtapose these rulings with the recent Case T-125/22 *RT France v Council*, ECLI:EU:T:2022:483 for a consistency check. In a groundbreaking decision, the General Court for the first time ruled on the Council of the European Union's restrictive measures designed to prohibit the dissemination of audiovisual content. These measures, enacted on March 1, 2022, followed Russia's military assault on Ukraine on February 24, 2022. The goal was to temporarily suspend the propaganda related to the military action through certain Russian-controlled media outlets. Consequently, EU operators were barred from broadcasting content produced by listed entities, including the applicant RT France, who sought annulment based, *inter alia*, on its freedom of expression and information and freedom to conduct a business. The CJEU rejected the request on both grounds by concluding that, given the temporary and reversible nature of the measures, they did not disproportionately infringe on the applicant's freedoms of expression and business. The court further noted that the measures still allowed the applicant to engage in other forms of media distribution like investigations and interviews, thus respecting the essence of the right to freedom of expression.
[144]Ibid.; *Bulgakov*, see n. 141, para. 34.
[145]Ibid., para. 30.
[146]Ibid.
[147]*Engels*, see n. 142, para. 29.

Shortcomings identified by the ECtHR include the broad discretion to impose blocking measures afforded by law to an executive agency, causing content to be blocked arbitrarily and excessively. Therefore, the powers of state authorities must be clearly circumscribed to minimise the impact of such measures on Internet access.[148] The ECtHR also drew attention to the lack of procedural guarantees, notably, the absence of court orders sanctioning blocking measures, impact assessments prior to implementation, advance notification to affected parties and proportionality assessments in court decisions subsequent to implementation of blocking measures.[149]

The ECtHR issued guidance on potential public interest issues that could arise due to the actions of DSPs. The extent of potential limitations to freedom of expression have been highly content dependent, with courts applying different balancing standards, based on the nature of the content to be moderated. In *Akdeniz*, the ECtHR confirmed that in cases with a high public interest, blocking online information may not be compatible with Article 10 ECHR. The public interest test is not only applicable to political information and has been recognised, albeit to a stricter standard,[150] in sporting matters,[151] performing artists,[152] to material relating to the moral position of an influential religious community[153] and other 'civil' expressions. Besides special protection afforded to public interest matters, political speech receives the highest level of protection. *Akdeniz* reiterated that Article 10(2) of the Convention does not allow much leeway for restrictions of freedom of expression in political matters.[154] With little scope for restrictions on political speech, the limits of acceptable criticism are wider regarding politicians, who knowingly open themselves to close scrutiny.[155] Closely related to political speech, satire also enjoys a high level of protection.[156] The ECtHR refers to satire as 'a form of artistic expression and social commentary which, by its inherent features of exaggeration and distortion of reality, naturally aims to provoke and agitate. […] any interference with the right of an artist – or anyone else – to use this means of expression should be examined with particular care'.[157] Satire requires contextualisation and it should be examined in the light of the case as a whole, particularly with regard to the status of the person at whom it was directed, the alleged offender's own position, its form and the context.[158] From the perspective of content moderation practices, a high level of protection granted to these types of content should equate to few instances of their authorised and lawful removal.

Even though in practice the line between political speech, satire and defamatory content is often rather thin, only the latter qualifies as unlawful speech.[159] In this context, the CJEU found that the 'injunction must be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal'.[160] However, differences in wording must not 'be such as to require the host provider concerned to carry out an independent assessment of that content'.[161] Instead, the ECtHR case law regarding offensive, vulgar or defamatory content,[162] endorsed a rather more narrow approach as the removal of comments that do not amount to hate speech

[148] *Kharitonov*, see n. 139, paras 38, 43.
[149] ibid, paras 43, 45.
[150] See D. Harris and others, *Harris, O'Boyle, and Warbrick: Law of the European Convention on Human Rights* (OUP 2009), 457.
[151] See *Nikowitz and Verlagsgruppe News GmbH v Austria* App. no. 5266/03 (ECtHR, 22 February 2007), para 25 (society's attitude towards a sports star); *Colaço Mestre and SIC—Sociedade Independente de Comunicação, SA v Portugal* App. nos 11,182/03 and 11,319/03 (ECtHR, 26 April 2007), s 28 (an interview by the president of the sports club); *Ressiot and Others v France* App. nos 15,054/07 and 15,066/07 (ECtHR, 28 June 2012), para 116 (doping practices in professional sport).
[152] See *Sapan v Turkey* App no 44102/04 (ECtHR, 8 June 2010), para 34 (a book about a Turkish pop star).
[153] See *Verlagsgruppe News GmbH and Bobi v Austria* App. no. 59631/09 (ECtHR, 4 December 2012), para 76.
[154] *Akdeniz*, see n. 120, para. 28.
[155] *Lindon, Otchakovsky-Laurens and July v France* App. Nos. 21,279/02 and 36,448/02 (EctHR, 22 October 2007), para. 46.
[156] *Eon v. France* App. no. 26118/10, (ECtHR, 14 March 2013).
[157] Ibid., para. 60.
[158] Ibid., para. 53.
[159] *Delfi AS v Estonia* App. no. 64569/09 (ECtHR, 16 June 2015) (hereafter '*Delfi*'), para. 110.
[160] *Glawischnig-Piesczek*, see n. 60, para. 41.
[161] ibid, para. 45.
[162] *Magyar Tartalomszolgáltatók Egyesülete and Index.Hu v Hungary* App. no. 22947/13 (ECtHR, 2 May 2016) (hereafter '*MTE*'), para. 64 (offensive and vulgar comments which do not constitute clearly unlawful speech); *Høiness v. Norway*, App. no. 43624/14 (ECtHR, 19 March 2019), para 69 (tasteless and vulgar comments, not necessary to examine in depth their nature, as they in any event did not amount to hate speech or incitement to violence); *Pihl v. Sweden* (dec.) App. no. 74742/14 (ECtHR, 7 February 2017) (hereafter '*Pihl*'), para. 25 (defamatory comment).

or an incitement to violence does not require the use of automated proactive monitoring.[163] The ECtHR outlined that expecting a platform to assume that some unfiltered comments might be in breach of the law would amount to requiring excessive and impractical forethought capable of undermining the right to impart information via the Internet.[164] For example, in *Høiness v. Norway*, Hegnar Online, a large commercially-run news portal with popular forums, where defamatory content was posted, complied with its obligations by establishing a moderation system allowing users to report content and by using other ex post control measures.[165] Instead, the ECtHR considers it necessary 'to sanction or even prevent all forms of expression which spread, incite, promote or justify hatred based on intolerance […], provided that any 'formalities', 'conditions', 'restrictions' or 'penalties' imposed are proportionate to the legitimate aim pursued'.[166] Similarly, certain forms of expression, such as content denying crimes against humanity and established historical facts, for example the Holocaust, cannot be protected under Article 10 ECHR, due to Article 17 ECHR prohibiting the abuse of rights.[167] Therefore, all these forms of expression should be removed with little, if any, restrictions. This strict approach has been confirmed in the case of *Delfi AS v. Estonia*, concerning the delayed removal of online comments containing 'odious hate speech and speech inciting violence'.[168] Unprotected speech also includes child abuse and, most likely, terrorist propaganda.[169] The mechanism put in place by *Delfi*, an online news portal, to filter comments consisted of four measures, including an automatic filtering tool.[170] The ECtHR concludes that:

> the automatic word-based filter used by [Delfi] failed to filter out odious hate speech and speech inciting violence posted by readers and thus limited its ability to expeditiously remove the offending comments. […] Thus, even if the automatic word-based filter may have been useful in some instances, […] it was insufficient for detecting comments whose content did not constitute protected speech under Article 10 of the Convention.[171]

Consequently, in order to comply with Article 10 ECHR, *Delfi* was not only obliged to use an automatic filtering system, but such a system should have been efficient enough to filter out specific types of content.[172]

Contrary to hate speech, while copyright protected content supposedly enjoys the protection provided to the fundamental right to property,[173] this right is not absolute. As a result, the rights of copyright holders have to be balanced against other fundamental rights. In the cases of *Netlog*[174] and *Scarlet*,[175] users' freedom to receive or impart information was taken into consideration in a balancing exercise regarding copyright protected content. The CJEU

[163] *MTE*, see n. 162, para. 91; *Pihl*, see n. 162.

[164] *MTE*, see n. 162, para. 82; *Pihl* (n 162) para. 31.

[165] *Høiness v Norway* App. no. 43624/14 (ECtHR, 19 March 2019). paras 70–73 (unlike in *Delfi*, mentioned below, the defamatory comments to delete did not amount to hate speech or speech inciting violence).

[166] *Erbakan v Turkey*, App. no. 59405/00, (ECtHR, 6 July 2006). Para. 56.

[167] *Garaudy v France* (dec.), App. no. 65831/01, (ECtHR, 24 June 2003) (concerning the Holocaust). The Court clarified that Art 17 ECHR should be resorted to if the impugned speech sought to deflect Art 10 ECHR from its real purpose 'by employing the right to freedom of expression for ends clearly contrary to the values of the Convention'. See *Perinçek v Switzerland* App no 27510/08 (ECtHR, 15 October 2015). Para. 114.

[168] *Delfi*, see n. 159, para. 156.

[169] See, e.g., Mouvement raëlien suisse v. Switzerland, *App. no. 16354/06* (ECtHR, 13 July 2012) (banning a campaign, whose ideas 'might lead to sexual abuse of children by some of its members'); *Karttunen v Finland* App no 1685/10 (ECtHR, 10 May 2011) (recognising limitation to the freedom of arts in case of photographs displaying child abuse and pornography); *Delfi*, see n. 159, para 48 (reminding that, inter alia 'legitimate types of information which may be restricted include child pornography (to protect the rights of children)'); *Roj TV A/S v Danemark* (dec) App no 24683/14, (ECtHR, 17 April 2018) (concluding terrorist-related expressions advocating the use of violence, and the repetitive incitement to participate in fights and actions, do not attract Freedom of Expression protection); *Sabuncu and Others v. Turkey* App no 23199/17 (ECtHR, 10 November 2020) (banning speech that justifies the commission of terrorist offences). In this context, however, it is worth highlighting that acts such as documenting war crimes should be protected and how tension with regards to content moderation efforts could arise, as the latter type of content could be wrongfully removed for being considered as terrorist propaganda.

[170] More specifically, it included: (i) disclaimers (on accountability for comments and prohibition of comments contrary to good practices), (ii) an automatic system of deletion of comments based on stems of certain vulgar words, (iii) a notice-and-take-down system, as well as (iv) practice to remove inappropriate comments by administrators on their own initiative.

[171] ibid, para. 156.

[172] Ibid., para. 110.

[173] Article 17 Charter and Article 1 of Protocol No. 1 ECHR.

[174] *Netlog*, see n. 54.

[175] *Scarlet*, see n. 54.

found that an injunction requiring the hosting service provider to install a filtering system would upset the fair balance in favour of copyright holders.[176] Actually, the introduction of automated filtering systems applied by DSPs could lead to lawful communications being blocked as these systems may not distinguish adequately between unlawful content and lawful content covered by statutory copyright exceptions, public domain works and those posted online free of charge by their authors.[177]

In sum, any platform liability regime should prioritise a user-centric approach that upholds the fundamental rights of freedom of expression and access to information. Regulation must be precise, legally certain, and incorporate procedural safeguards to avoid blanket content restrictions. Terms that are too broad could leave too much discretion to the authorities and make the application of a legal instrument unforeseeable.[178] Any restrictions imposed on digital platforms should not disproportionately interfere with users' fundamental rights. For instance, wholesale blocking of entire websites often disregards the legal content present, thereby violating the essence of freedom of expression.[179] Otherwise, restrictions could result in a violation of Article 10 ECHR and—by extension and analogy— Article 11 EU Charter. Importantly, the platform's policies should be sensitive to the nature of the content, with heightened protections for public interest matters and political discourse, while rigorously sanctioning hate speech and other illegal forms of expression. As the nature of content matters, platforms should aim for granularity in content moderation, recognising the different standards that apply based on the type of content. To that end, the DSA implementation process should clearly define notions incorporated in the DSA. and content that platforms might be under the obligation to remove.

3.1.2 | Freedom of expression, freedom to impart information and freedom of the arts

The freedom to impart information must be considered alongside the rights that are balanced in an intermediary liability regime. Freedom of the arts has recently been invoked more often by the legislator and the CJEU. In its resolution on the DSA and FRs, the EP explicitly invokes Article 13 EU Charter.[180] Freedom of the arts falls within the scope of freedom of expression, enshrined in Article 11 EU Charter and Article 10 ECHR, and 'affords the opportunity to take part in the public exchange of cultural, political and social information and ideas of all kinds'.[181] In the context of a creative reuse of a small portion of a song via sampling, the CJEU balanced IP rights against freedom of the arts and other fundamental rights.[182] In his Opinion in *YouTube/Cyando*, the Advocate General refers to freedom of the arts and outlines:

> the fundamental rights of users of those platforms cannot be ignored. These include freedom of expression and information [...] It is clear from the case-law of both the Court of Justice and the European Court of Human Rights that the internet is of particular importance in this respect. More specifically, the latter court has held that YouTube is an important means by which individuals exercise that freedom. That is also the case for freedom of the arts, which is guaranteed by Article 13 of

[176] *Netlog*, see n. 54, para 51; *Scarlet*, n. 54, para. 53.

[177] *Netlog*, see n. 54, para 50; *Scarlet*, n. 54, para. 52.

[178] See for example, *Karastelev and Others v Russia* App. no. 16435/10 (ECtHR, 6 October 2020). The case concerned public protests against a law requiring, among other things, minors to be accompanied by an adult in public places at night. The Russian authorities had found that a poster displayed during a protest against the law and encouraging adolescents to participate in further protests had amounted to planning an 'extremist activity' under the Russian legislation. Terms such as an 'extremist activity', 'extremist nature' were found to be too broad by the ECtHR.

[179] In this context, European Commissioner for Internal Market Thierry Breton has recently clarified that internet shutdowns and social media blockings are not lawful under the Digital Services Act (DSA), except under extreme and clearly-established "last resort" circumstances. See, e.g., 'DSA is not a censorship tool: Commissioner Breton must clarify blocking statement' (Accessnow, 3 August 2023) <https://www.accessnow.org/press-release/dsa-internet-blocking>.

[180] EP Resolution on the DSA and FRs, see n. 93.

[181] C-476/17 *Pelham GmbH and Others v. Ralf Hutter and Florian Schneider-Esleben*, EU:C:2019:624, para 34.

[182] Ibid.

> the Charter and is closely linked to freedom of expression, given the large number of people using online platforms such as YouTube to share their creations online.[183]

Moreover, in *Funke Medien* and *Spiegel Online*, both concerning the interaction between copyright protection and media freedom, the CJEU unequivocally characterised 'exceptions and limitations' to copyright as user rights.[184] Such a development bears important consequences for the enforceability of copyright 'exceptions and limitations', which should no longer be understood as mere defences to infringement, but might be deemed enforceable, for example, vis-à-vis Terms of Service that impose additional restrictions on the legislatively envisaged 'exceptions and limitations' to copyright.[185]

Three questions are of essence in looking for proper equilibrium between these users' rights, freedom of expression and liability regimes: the impact of the type of liability regime, the impact of algorithmic enforcement, and the impact of blocking orders.

First, the CJEU has discussed at length the impact of different liability regimes on multiple fundamental rights, including freedom of expression. In the case of *Google v Louis Vuitton*, the Advocate General of the CJEU stated that the rules of civil liability, based on the law of negligence, were more suited to the regulation of DSPs than the strict liability rules of IP law. The Advocate General stated, in the case of online trademark infringement:

> [l]iability rules are more appropriate, since they do not fundamentally change the decentralised nature of the internet by giving trade mark proprietors general—and virtually absolute—control over the use in cyberspace of keywords which correspond to their trade marks. Instead of being able to prevent, through trade mark protection, any possible use—*including, as has been observed, many lawful and even desirable uses*—trade mark proprietors would have to point to specific instances giving rise to Google's liability in the context of illegal damage to their trademarks.[186]

Further, the Advocate General argued that a negligence-based system would be best placed to strike a balance between IP rights, access to information, and freedom of expression. Incidentally, the ECD requires online intermediaries to respect the right of freedom of expression when considering a takedown request.[187] Although the takedown system is far from perfect, it does provide a safeguard for the right to freedom of information providing the intermediaries are forced to properly consider the infringing material before a takedown.

Second, *ex ante* mechanisms, based on the filtering and automated content moderation- systems, potentially give strong pre-eminence to IP rights over other rights, as the case law of the CJEU has emphasised. As already mentioned, the CJEU explained that the measures 'could potentially undermine freedom of information, since [automated systems] might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications'.[188] In *YouTube/Cyando*, the Advocate General emphasised that '[r]equiring online platform operators to check, in a general and abstract manner, all the files which

[183]C-682/18 *LF v. Google LLC, YouTube Inc., YouTube LLC, Google Germany GmbH and C-683/18 Elsevier Inc. v. Cyando AG, ECLI:EU:C:2020:586*, Opinion of AG Saugmandsgaard Øe, para 241 (hereafter '*YouTube/Cyando* AG Opinion').

[184]As stated by the CJEU in *Funke Medien* and *Spiegel Online*, 'although Article 5 of Directive 2001/29 is expressly entitled "exceptions and limitations", it should be noted that those exceptions or limitations do themselves confer rights on the users of works or of other subject matter'. See C-469/17 *Funke Medien NRW GmbH v Bundesrepublik Deutschland*,ECLI:EU:C:2019:623, para. 70 and C-516/17 *Spiegel Online GmbH v Volker Beck*,ECLI:EU:C:2019:625, para. 54. For further discussion, see also C. Geiger and E. Izyumenko, 'The Constitutionalization of Intellectual Property Law in the EU and the Funke Medien, Pelham and Spiegel Online Decisions of the CJEU: Progress, But Still Some Way to Go!', (2020) 51(3) *IIC*, 282; C. Geiger and E. Izyumenko, 'Freedom of Expression as an External Limitation to Copyright Law in the EU: The Advocate General of the CJEU Shows the Way', (2019) 41(3) *EIPR*, 131 (including further references). This position is however not new, as the CJEU had already recognised user rights based on fundamental rights in its judgments Telekabel, see n. 120, para. 57 and C-117/13 *Technische Universität Darmstadt v Eugen Ulmer KG*, EU:C:2014:2196, para. 43.

[185]See Geiger and Izyumenko, 'Blocking Orders', see n. 137, 570.

[186]C-236–238/08 *Google France, SARL & Google Inc. v Louis Vuitton Malletier SA, Viaticum SA, Luteciel SARL v Centre Bational de Recherche en Relations Humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger, a franchisee of Unicis*, ECLI:EU:C:2009:569, AG's Opinion, para. 123.

[187]See Directive 2001/29/EC, see n. 72, Recital 46.

[188]*Netlog*, see n, 54, para. 50.

their users intend to publish before they are uploaded in search of any copyright infringement would introduce a serious risk of undermining these different fundamental rights'.[189]

Providing maximum protection for certain forms of intellectual creativity through the deployment of filtering technologies that are not able to distinguish between legal and illegal uses of content might undermine other forms of creativity which are also positive for society, thus infringing Article 13 EU Charter.[190] Currently, the technology used to regulate infringing material lacks the capability to make accurate decisions and can lead to false positives that could restrict users' fundamental right of freedom of expression. Technology is unable to replicate human judgement in scenarios where fair use or copyright limitations apply, therefore case-by-case analysis is needed to protect fundamental rights.[191] Further, technologies designed to identify infringing content are unable to deal with the complexities surrounding public domain status of works.[192] Moreover, in order to keep pace with technology advancements, 'external and/or open-ended copyright exceptions (such as the freedom of expression-grounded 'fair use' or open exceptions akin to the German 'free use' which the CJEU outlawed in *Pelham*) are [argued to be] necessary for the proper functioning and balanced construction of copyright law in the EU'.[193] The potential to program open ended limitations into an algorithm is even more challenging due to their flexibility as a legal standard.[194] In this scenario, the use of algorithmic tools will pose even more risks to freedom of arts and expression more generally. In this context, Article 17 of the C-DSM Directive[195] raises fundamental questions regarding the preservation of users' freedom of expression and information due to the increase in general monitoring of uploaded content by online platforms and the use of automatic infringement-assessment systems that the reform might cause.[196]

Third, the courts have also acknowledged that the blocking of websites involves the right of freedom of expression of Internet service providers.[197] This has been highlighted by the Advocate General in the case of *Telekabel*: '[a]lthough it is true that, in substance, the expressions of opinion and information in question are those of the ISP's customers, the ISP can nevertheless rely on that fundamental right by virtue of its function of publishing its customers' expressions of opinion and providing them with information'.[198] The Advocate General made reference to an ECtHR precedent which provided that 'Article 10 guarantees freedom of expression to "everyone", [with] [n]o distinction [being] made in it according to the nature of the aim pursued or the role played by natural or legal persons in the exercise of that freedom'.[199] Further, the ECtHR noted that although 'publishers do not necessarily associate themselves with the opinions expressed in the works they publish, . . . by providing authors with a medium they participate in the exercise of the freedom of expression'.[200] DSPs' freedom of expression has been further discussed by

[189] *YouTube/Cyando* AG Opinion, see n. 183, para. 242.

[190] Ibid., para. 243.

[191] Furthermore, in the EU the manner in which the Member States implement even the same exceptions can vary considerably from country to country. E.g. a quotation exception has a very different scope across Europe. See B. Hugenholtz and M. Senftleben, 'Fair Use in Europe: in Search of Flexibilities', Institute for Information Law Research Paper no. 2012/33 (2012), 15–17. See also in this sense, C. Geiger and F. Schönherr, *Frequently Asked Questions (FAQ) of Consumers in relation to Copyright, Summary Report* (EUIPO 2017) <https://euipo.europa.eu/ohimportal/web/observatory/observatory-publications> (listing exceptions and limitations to copyright as one of the areas of major divergence in national copyright law). See ibid., 6–8.

[192] See *Netlog*, see n. 54, para. 50.

[193] Geiger and Izyumenko, see n. 184, 282. See also C. Geiger and E. Izyumenko, 'Towards a European 'Fair Use' Grounded in Freedom of Expression" (2019) 35(1) *AUILR* 1; C. Geiger, "Fair Use' through Fundamental Rights in Europe, When Freedom of Artistic Expression allows Creative Appropriations and Opens up Statutory Copyright Limitations' in S. Balganesh, W. Loon Ng-Loy and H. Sun (eds), *The Cambridge Handbook of Copyright Limitations and Exceptions, Cambridge* (CUP 2021), 174.

[194] See D. Burk, 'Algorithmic Fair Use', (2019) 86(2) *University of Chicago Law Review*, 290.

[195] See Directive 2019/790/EU, see n. 11.

[196] Many scholars have been highlighting this tension. See, e.g., M. Senftleben, J. P. Quintais and A. Meiring, 'Outsourcing Human Rights Obligations and Concealing Human Rights Deficits: The Example of Monetizing User-Generated Content Under the CDSM Directive and the Digital Services Act', (2023) SSRN Research Paper 4,421,150/23, 11–19 <https://ssrn.com/abstract=4421150>; Frosio, see n. 87, 709–750; Geiger, Frosio and Izyumenko, see n. 43, 146; G. Frosio and S. Mendis, 'Monitoring and Filtering: European Reform or Global Trend?' in Frosio (ed), see n. 1, 563–564; M. Senftleben, 'Bermuda Triangle—Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market', (April 2019) SSRN Research Paper no. 3367219 <https://ssrn.com/abstract=3367219>.

[197] See, on this issue extensively, Geiger and Izyumenko 'The Role of Human Rights in Copyright Enforcement Online', see n. 120, 43 ff.

[198] C-314/12 *UPC Telekabel Wien* [2013] ECLI:EU:C:2013:781, Opinion of AG Villalón, para 82 (hereafter '*Telekabel*, Opinion of AG Villalón').

[199] *Öztürk v Turkey* App. no. 22479/93 (ECtHR, 28 September 1999), para. 49.

[200] Ibid.

the ECtHR with mixed outcomes. In the case of *Delfi AS*,[201] the Grand Chamber of the ECtHR found that there was no infringement of Article 10. Conversely, in a recent decision, the ECtHR did rule that finding an ISP liable for the comments made by users ran contrary to the ISP's freedom of expression.[202]

To conclude, the quest for an equitable platform liability regime suggests that the equilibrium between freedom to impart information and freedom of the arts and other competing rights is both granular and subtle. First, a negligence-based liability system emerges as the most apt mechanism, upholding the decentralisation ethos of the internet while better respecting free expression and competing rights. Second, the adoption of algorithmic enforcement tools necessitates a judicious approach to safeguard against erroneous limitations on users' freedoms. Automated systems, if employed, must be highly efficient in distinguishing between illegal and legal content, particularly when balancing user freedoms against obligations like copyright enforcement. Overly aggressive automated filtering systems can lead to 'false positives', thus blocking lawful content and infringing on freedom of expression and information. Finally, the application of blocking orders implicates not just the rights of users but also the freedom of expression of Internet Service Providers, warranting judicious legal scrutiny.

3.1.3 | Right to respect for private life and data protection.

The right to freedom of expression is not the only fundamental right that must be taken into account when considering DSPs' regulation and content moderation practices. The right to respect of private life must be effectively balanced against competing rights.[203] The courts have also emphasised that imposing filtering and monitoring obligations on DSPs can lead to the infringement of users' privacy and personal data protection. The CJEU addressed this issue as follows: 'requiring installation of the contested filtering system would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users [which] is protected personal data because, in principle, it allows those users to be identified'.[204] In the cases of *Scarlet* and *Netlog*, the CJEU established, for the first time, the 'fundamental right to the protection of personal data, which is not fairly balanced with copyright holders' rights when a mechanism requiring the systematic processing of personal data is imposed in the name of the protection of intellectual property'.[205] Additionally, the ECtHR applies further scrutiny when a system monitors communications, and has considered that technologies that filter communications could infringe the right to respect for private life, particularly when automated systems are used.[206] Data protection was also upheld by the CJEU in the case of *Constantin Film*, in which the court ruled against the request to order YouTube and Google to disclose information of users allegedly infringing the film distributor Constantin Film's exclusive rights. The CJEU was called on to determine whether under Article 8(2)(a) ('right to information') of the Enforcement Directive (2004/48/EC) the term 'addresses' should be interpreted to including user's email address, telephone number and IP address. The CJEU limited the reach of IP enforcement by finding that the term 'addresses' covers only the postal address and does not refer to the email address, telephone number or IP address.[207]

[201]See *Delfi*, see n. 159.
[202]See *MTE*, see n. 162.
[203]See EU Charter, Art. 7.
[204]*Netlog*, see n. 54, para. 49.
[205]Gloria González Fuster, 'Balancing Intellectual Property Against Data Protection: a New Right's Wavering Weight', (2012) 14 *IDP Revista de Internet Derecho y Política*, 34, 37.
[206]See *Liberty v United Kingdom* App no 58243/00 (ECtHR, 1 July 2008), para 56; *S. and Marper v United Kingdom* App no 30562/04 (ECtHR, 4 December 2009), para 104–105; *Copland v United Kingdom* App no 62617/00 (ECtHR, 3 April 2007), para 41–44; *Malone v United Kingdom* App no 8691/79 (ECtHR, 2 August 1984), para 83–84. See also S. Kulk and F. Zuiderveen Borgesius, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2012) 34 *Europen Intellectual Property Review*, 791, 793–4.
[207]Case C-264/19 *Constantin Film Verleih GmbH v YouTube LLC, Google Inc*. ECLI:EU:C:2020:542, paras 28, 30, 39 (however, Member States can allow competent judicial authorities to order disclosure of all these users' information in proceedings concerning an infringement of an intellectual property right).

The right to be forgotten also implicates a fine balancing between competing fundamental rights as a result of monitoring and filtering obligations. The CJEU found, in 2014, that an Internet search provider has the responsibility for personal data it processes that appear on third party web pages.[208] As a result, search engines can be compelled to remove links to web pages that include personal data. The EU's recognition of the 'right to be forgotten' found criticism due to the fact that it could jeopardise the freedom of expression and access to information.[209] In fact, the CJEU stated that the right to privacy supersedes 'not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name'.[210] However, the CJEU continued by noting that the general rule should not apply in situations where there is large public interest in accessing the information 'for particular reasons, such as the role played by the data subject in public life'.[211]

The European Data Protection Authorities (DPAs), assembled in the, then, Article 29 Working Party (WP29),[212] adopted guidelines qualifying the *Google Spain* decision and including common criteria that national DPAs should employ when dealing with complaints. The WP29 seeks to find a balance between the nature and the sensitivity of data and the public interest in access to the information.[213] However, if the data subject is a public figure the public interest will be higher.[214] This means that the guidelines intrude very little on the rights to freedom of expression and access to information. The DPAs are only able to delist a web address if they assess that the rights of the data subject outweigh the public interest connotations.[215] Further, when dealing with complaints about the refusal to delist a web address, the national DPAs must apply thirteen key criteria that uphold 'the interest of the general public in having access to [the] information'.[216]

The national courts of EU Member States echoed the WP29 and clarified the balancing of personal privacy interest and public interest in access to information by ruling that the *Google Spain* decision 'does not intend to protect individuals against all negative communications on the Internet, but only against "being pursued" for a long time by "irrelevant", "excessive" or "unnecessarily defamatory" expressions'.[217] For example, information about a conviction for a serious crime would provide relevant information about an individual, thus cannot be delisted.[218] Again, the interest in promoting market transparency and protecting third parties would imply that the data included in a Commercial Registry 'cannot be cancelled, anonymized, or blocked, or made available only to a limited number of interested parties'.[219]

In sum, privacy and data protection rights might be a limitation to access to information and DSPs'—or rightsholders'—interest in processing data for monitoring and filtering purposes, however, according to EU law, public interest should always prevail.

[208]See C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317 (hereafter '*Google Spain*').

[209]See, e.g., M. Peguera, 'The Shaky Ground of the Right to Be Delisted', (2015) 15 *Vanderbilt Journal of Entertainment & Technology Law*, 507; J. Rosen, 'The Right to Be Forgotten', (2015) 64 *Stanford Law Review Online*, 88; S. Kulk and F. Zuiderveen Borgesius, 'Google Spain v. González: Did the Court Forget About Freedom of Expression?', (2014) 3 *European Journal of Risk Regulation*, 389; J. Zittrain, 'Don't Force Google to Forget' (*New York Times*, 14 May 2014) <http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0>. See also OSCE Representative on Freedom of the Media, Dunja Mijatović, 3rd Communiqué on Open Journalism, 29 January 2016, 2 <http://www.osce.org/fom/219391?download=true>; M. Taddeo and L. Floridi, 'The Debate on the Moral Responsibility of Online Service Providers', (2015) *Science and Engineering Ethics*,1, 18–19.

[210]*Google Spain*, see n. 208, para. 81.

[211]Ibid.

[212]The Article 29 Working Party is a short name for The Working Party on the Protection of Individuals with regard to the Processing of Personal Data, an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor, and the European Commission. Following the entry into force of the GDPR, the WP29 is now called European Data Protection Board (EDPB).

[213]Ibid. 2.

[214]Ibid.

[215]Ibid.

[216]Ibid. 11, 13–19.

[217]Rechtbank [District Court] Amsterdam [2014] ECLI:NL:RBAMS:2014:6118 (Neth.), as translated in J. Spauwen and J. van den Brink, 'Dutch Google Spain ruling: More Freedom of Speech, Less Right To Be Forgotten For Criminals (*Inforrm's Blog*, 27 September 2014) <https://inforrm.wordpress.com/2014/09/27/dutch-google-spain-ruling-more-freedom-of-speech-less-right-to-be-forgotten-for-criminals-joran-spauwen-and-jens-van.-den-brink>.

[218]Ibid.

[219]See C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*,ECLI:EU:C:2016:652, Opinion of AG Bot.

3.1.4 | Due process and fair trial

Due process is the principle that ensures laws and legal proceedings are fair, efficient, and effective and do not limit the basic rights of life, liberty and property.[220] Further, the principle of due process relies on the right to a fair trial, which can only be granted when parties have access to 'a competent, independent and impartial tribunal' that recognises a number of human rights conventions.[221] The right of access to a court must be 'practical and effective'.[222] In order to be effective, an individual must have 'a clear, practical opportunity to challenge an act that is an interference with his rights'.[223] The length of proceedings before domestic courts could render such a right ineffective, in particular, content shared by a user may lose its relevance and become outdated if the proceedings are extensively lengthy. Even if the final decision is favourable, that may not be sufficient to remedy the damage sustained.

The principle of equality of arms also stems from the right to fair trial. Under the case-law of the ECtHR, equality of arms is understood as a 'fair balance' between the parties,[224] it implies that each party must be afforded a reasonable opportunity to present their case under conditions that do not place either party at a substantial disadvantage.[225] Significant advantages as regards access to relevant information of one party, in most cases an online platform, may lead to an imbalance detrimental to the other party, most often a user, that is incompatible with the principle of equality of arms.[226]

Algorithmic decision-making, increasingly implemented by DSP's content moderation practices, poses obvious challenges to due process and related fundamental rights.[227] In the IP domain and elsewhere, socially relevant choices online increasingly occur through automated private enforcement run by opaque algorithms, creating a so-called 'black-box' society.[228] It has even been argued that the use of algorithmic enforcement by DSPs shows a shift in the governance by 'law enforcement and adjudication powers in the hands of a small number of mega platforms, which are profit-maximising, and possibly biased, private entities'.[229] Algorithmic enforcement focuses on the detection and prevention whilst leaving the prosecution to the DSPs, whereas the traditional method of enforcement involves multiple public authorities taking charge of each step of enforcement.[230] Algorithmic enforcement therefore potentially affects due process principles by removing the 'trust and accountability that are inherent to reliable systems of law enforcement'.[231]

There are three main due process concerns that arise from algorithmic enforcement: (1) transparency, (2) accountability and (3) contestability. First, transparency is the availability of the methods and processes behind a decision.[232]

[220]See A. Denning, *Due Process of Law* (OUP 1980).

[221]See, e.g., Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) (hereafter 'UDHR') art 10; ECHR, see n. 116, art 6; Charter, see n. 116, art 47–50 (providing at Article 47(2) that everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law). The scope of these rights is not limited to the listed above provisions, but it is incorporated, in particular, through jurisprudence of the CJEU and the ECtHR, in various other provisions in the form of procedural obligations.

[222]*Bellet v France* App. no. 23805/94 (ECtHR, 4 December 1995) (hereafter '*Bellet*'), para 38; *Zubac v. Croatia* App. no. 40160/12 (ECtHR, 5 April 2018), paras 76–79; European Court of Human Rights, Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (civil limb) (*ECHR*, 2019) <https://www.echr.coe.int/Documents/Guide_Art_6_ENG.pdf> (hereafter 'ECHR Guide on Article 6').

[223]*Bellet*, see n. 222, para 36; *Nunes Dias v Portugal* (dec.) App. nos. 2672/03 and 69,829/01 (ECtHR, 10 April 2003), ECHR Guide on Article 6 (n. 222).

[224]*Feldbrugge v the Netherlands* App. no. 8562/79 (ECtHR, 29 May 1986), para. 44.

[225]*Regner v the Czech Republic*, App. no. 35289/11 (ECtHR,19 September 2017), para. 146; *Dombo Beheer B.V. v the Netherlands*, App. no. 14448/88 (ECtHR, 27 October 1993), para 33; ECHR Guide on Article 6, see n. 222; Felipe Romero-Moreno, '"Notice and staydown" and social media: amending Article 13 of the Proposed Directive on Copyright', (2019) 33(2) *Computers & Technology*, 187–210.

[226]*Yvon v France* App. no. 44962/98 (ECtHR, 24 April 2003), para. 37.

[227]See, for an introductory overview, Frosio, see n. 24, 709–744.

[228]See Pasquale, see n. 33. See also N. Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (CUP 2019); T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018).

[229]M. Perel and N. Elkin-Koren, 'Accountability in Algorithmic Copyright Enforcement' (2016) 19 *Stanford Technology Law Review*, 473, 473.

[230]Ibid., 481.

[231]Ibid.

[232]See Council of Europe, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT), 'Draft Recommendation of the Committee of Ministers to member States on human rights impacts of algorithmic systems' [12 November 2018] MSI-AUT(2018)06, 6–7 <https://rm.coe.int/draft-recommendation-on-human-rights- impacts-of-algorithmic-systems/16808ef256>; A. Koene et al, *A governance framework for algorithmic accountability and transparency* (European Parliament Research Center 2019) 4–8; A. Rieke, M. Bogen, and D. Robinson, *Public Scrutiny of Automated Decisions: Early Lessons and Emerging Methods* (An Upturn and Omidyar Network Report, 2018), 23–28 <https://www.issuelab.org/resources/30226/30226.pdf>.

Second, accountability refers to taking responsibility for the decision.[233] Third, contestability is the power to dispute the results of an automated enforcement decision.[234] These three requirements form the backbone of a fair judicial process. However, without transparency neither accountability nor contestability can be guaranteed.[235] The criteria for removing content or for blocking specific websites often remain secret.[236] The same is true for algorithms engaged in filtering of content. Therefore, interested parties call for more transparency[237] and accountability in relation to algorithms. There are a number of barriers in the way of a transparent algorithmic enforcement process. First, algorithmic system transparency could be limited by trade secrets or confidential information.[238] Secondly, public authorities may be prevented from revealing the decision-making process due to state secrets.[239] Thirdly, technical reasons may make it too complex to qualify the reasons for a certain decision, for example in case of fast-learning neural networks. It may thus be extremely difficult to determine which factors contributed to the decision.

To remedy the concerns above, due process safeguards must be embedded in algorithmic enforcement mechanisms established by DSPs, taking into consideration what is feasible and sustainable. Guidance might be found in international fundamental rights covenants to ensure that DSPs provide users with access to a prompt, transparent and effective review for their complaints, and provide for effective remedies, including content restoration and compensation for damages.[240] Principle 27 of the UN Guiding Principles on Business and Human Rights ('UN Guiding Principles') imparts a duty to make 'effective and appropriate non-judicial grievance mechanisms' available.[241] Further, under Principle 28 of the UN Guiding Principles, states should consider ways to facilitate access to effective non-state-based grievance mechanisms, for example mechanisms developed by online platforms. Although these mechanisms are non-judicial, they may still use adjudicative, dialogue-based or other culturally appropriate and rights-compatible processes. In this respect, the duty of states is not purely limited to establishing accessible state judicial systems, but also raising awareness of, or otherwise facilitating access to, non-state-based grievance mechanisms.[242] Likewise, the CoE's Committee of Ministers recommend that states should encourage appropriate self-regulatory frameworks or the development of co-regulatory mechanisms.[243]

Non-state-based grievance mechanisms may offer some benefits over state-based mechanisms such as speed of access and remediation, reduced costs, and transnational reach.[244] Compared to domestic courts, non-state mechanisms may impose few requirements regarding time limits or evidence. However, these mechanisms often lack impartiality in the decision-making due to the lack of independence of DSPs' employees entrusted with dispute resolution, as their salaries, promotions or dismissals may depend entirely on the outcome of the proceedings. They may also be inclined to minimise the damage caused to users due to corporate solidarity or simply lack of knowledge and

[233]See Perel and Elkin-Koren, see n. 229, 481–484; Koene et al, see n. 232, 8; R. Binns, 'Algorithmic Accountability and Public Reason', (2018) 31 *Philosophy & Technology*, 543, 543–556.

[234]See Council of Europe, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT), 'Draft Recommendation of the Committee of Ministers to Member States on human rights impacts of algorithmic systems' [12 November 2018] MSI-AUT(2018)06, 6–7 <https://rm.coe.int/draft-recommendation-on-human-rights-impacts-of-algorithmic-systems/16808ef256>.

[235]See, e.g., for a discussion of the link between transparency and contestability, Case C-817/19, see n. 37.

[236]See R. F. Jørgensen and A. Møller Pedersen, Chapter 10, 'Online Service Providers as Human Rights Arbiters in The Responsibilities of Online Service Providers' in M. Taddeo and L. Floridi (eds), *The Responsibilities of Online Service Providers* (Springer International Publishing AG 2017), 183.

[237]See L, Rainie and J, *Anderson, Code-Dependent: Pros and Cons of the Algorithm Age* (*Pew Research Center*, 8 February 2017) <https://www.pewresearch.org/internet/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/pi_2017-02-08_algorithms_0-01/>; Council of Europe, Algorithms and Human Rights: Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications, prepared by the Committee of Experts on Internet Intermediaries (MSI-NET) (March 2018), 37.

[238]See, e.g., M. Maggiolino, 'EU Trade Secrets and Algorithmic Transparency', (2019) Bocconi Legal Studies Research Paper No. 3363178 <papers.ssrn.com/sol3/papers.cfm?abstract_id = 3,363,178>; R. Wexler, 'Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System', (2018) 70 *Stanford Law Review*, 1343, 1343–1429; T. Moore, *Trade Secrets and Algorithms as Barriers to Social Justice* (Center for Democracy and Technology 2017).

[239]See J. Kroll and others, 'Accountable Algorithms', (2017) 165 *University of Pennsylvania Law Review*, 633, 658; Wexler, see n. 238, 1367.

[240]Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, 7 March 2018, points 1.3.10., 1.5.2.

[241]United Nations, Office of the United Nations High Commissioner for Human Rights, 'Guiding Principles on Business Human Rights: Implementing the United Nations "Protect, Respect, and Remedy" Framework' (2011) A/HRC/RES/17/4.

[242]ibid, Commentary on Principle 28.

[243]Recommendation CM/Rec(2018)2, see n. 240, point 1.3.10.

[244]Guiding Principles, see n. 241, Commentary on Principle 28.

training to decide on content removal. Various layers of transparency could be looked into, such as independent oversight mechanisms, reporting requirements, standardisation or certification practices as they could serve as a means for ensuring that States and businesses comply with their respective fundamental rights obligations as well as for assessing the processes and procedures put in place by States and businesses to that end.[245] In particular, the success of non-state mechanisms is dependent on measures taken by DSPs to ensure the independence of the mechanism. In the absence of independent oversight, it will be impossible to verify if internal rules are applied consistently, with emphasis on potential discriminatory treatment.

In order to achieve this, Facebook recently created an Oversight Board,[246] to act as a supplementary forum to challenge the removal of content on Facebook and Instagram with the power to overrule decisions made by content moderators or executives. As the Oversight Board is composed of renowned experts, including former judges, its decisions should be more impartial and motivated. Nevertheless, critics argue that the Oversight Board essentially establishes a system of private "justice" and "ordering", creating a stark contrast to the public justice system.[247] While some may defend this setup by pointing to arbitration as a similarly privatised model of dispute resolution, the comparison falters when considering the significant power imbalance between individual users and a tech behemoth like Facebook. Arbitration often involves parties with relatively comparable standing, but here, the scales are tilted severely. That's why people generally resort to the public justice system, which is built to be a neutral arena with checks and balances. Proponents of the Oversight Board might counter that even if the Board's rulings are unfavorable to users, these decisions can be contested before a court for a manifest breach of fundamental rights. However, this rebuttal assumes that the average user has the resources and legal acumen to engage in what could be a protracted and costly legal battle. As a further limitation, the number of disputes the Oversight Board will be able to resolve will likely remain rather low compared to the number of pieces of content removed by Facebook on a daily basis.[248] Therefore, while the Oversight Board is a step toward impartiality and checks on corporate power, its limitations make it an insufficient replacement for traditional, public avenues of justice.

Protection of user rights does not only depend on dispute resolution mechanisms. Legislation should provide for safeguards that allow users to effectively complain about decisions, actions, or inaction of DSPs. First, a notification about actions to be undertaken would be an essential tool to guarantee users' right to a legal remedy.[249] According to Mostert, 'digital due process' should be based on the following principles: (1) a fair and public review by an independent and impartial panel or competent court within a reasonable time; (2) a proper prior notification of the review; (3) an opportunity for a user or notifier to respond and present evidence in respect of a takedown or a stay-up inaction by a platform; (4) the right to legal representation; (5) the right to appeal to an appeals panel, alternative dispute resolution tribunal or competent court; (6) notifiers may at any stage in the process seek access to competent courts; (7) the right to receive a decision which clearly articulates the reason for that decision; and (8) the right

[245]L. McGregor, D. Murray and V. Ng, 'International Human Rights Law as a Framework for Algorithmic Accountability', (2019) 68 *International and Comparative Law Quarterly*, 309, 331.

[246]N. Clegg, 'Welcoming the Oversight Board' (*Facebook*, 6 May 2020) <https://about.fb.com/news/2020/05/welcoming-the-oversight-board/>.

[247]See, e.g., Speech by President of the European Commission von der Leyen at the European Parliament Plenary on the inauguration of the new President of the United States and the current political situation, Brussels, 20 January 2021, <https://ec.europa.eu/commission/presscorner/detail/en/speech_21_167> (noting, in response to the Oversight Board's upholding of former President Trump Facebook account's suspension following the infamous attack on the Capitol Building in Washington, D.C., that "[n]o matter how right it may have been for Twitter to switch off Donald Trump's account five minutes after midnight, such serious interference with freedom of expression should be based on laws and not on company rules. It should be based on decisions of parliaments and politicians and not of Silicon Valley managers").

[248]Facebook's oversight board acknowledges this limitation, and therefore selects cases that 'have the potential to affect lots of users around the world, are of critical importance to public discourse or raise important questions about Facebook's policies'. See 'Announcing the Oversight Board's first cases and appointment of trustees' (Oversight Board, December 2020) <https://www.oversightboard.com/news/719406882003532-announcing-the-oversight-board-s-first-cases-and-appointment-of-trustees>.

[249]Article 47 (1) EU Charter and Article 13 ECHR. See Joined Cases 203/15 and 698/15 *Tele2 Sverige AB v Postochtelestyrelsenk and Secretary of State for the Home Department v Tom Watson*, ECLI:EU:C:2016:970, para. 100. Moreover, in *Barbulescu v. Romania*, the ECtHR agreed that in the absence of prior warning to the claimant advising him that his Internet usage was being monitored, he still had a reasonable expectation of privacy. See *Barbulescu v Romania* App. no. 61496/08 (ECtHR, 5 September 2017), para. 133. See also Romero-Moreno, see n. 225, 187–210.

to an effective remedy including, for example, stay-up or takedown of the content.[250] These principles adapt safeguards and guarantees developed by the CJEU and the ECtHR to the digital world.

In summary, a robust platform liability regime should be anchored in the principles of due process, ensuring fair and impartial dispute resolution with practical access to justice. It must foster transparency, accountability, and contestability, particularly in algorithmic decision-making, with the implementation of 'digital due process' principles, including a fair public review, proper prior notification, the opportunity for users to present evidence, the right to legal representation, the right to appeal, and the right to an effective remedy. To address power imbalances, the system should advocate for the 'equality of arms' between platforms and users, so that any significant advantage in terms of access to relevant information should be balanced. Both state-based and non-state grievance mechanisms have roles to play, provided they meet standards of impartiality and effectiveness. Legislative safeguards and independent oversight are also crucial to ensure that these principles are not just theoretical but are effectively implemented in practice. Emphasising its role as a cornerstone in this context, the DSA has already laid down the essential legal norms that serve as a blueprint for actualising these guiding principles, details of which will be elaborated in Section 4. What remains crucial now is the effective and timely practical implementation of these norms to regulate complaint mechanisms within DSPs, secure unequivocal access to domestic courts for all parties, and, in particular, ensure that procedural safeguards designed to protect users are not just included but are stringently enforced by an independent authority or other initiatives led by the European Commission, such as the European Centre for Algorithmic Transparency.[251]

3.2 | Scope and normative content of the fundamental rights of platforms: freedom to conduct business and its implications

The fundamental right of freedom to conduct business must also be considered when imposing obligations on DSPs.[252] The freedom to conduct business has been recognised by the EU Charter, making this right young compared to the constitutionally established freedom of expression.[253] While it has been stated that 'to date the case law has not […] provided a full and useful definition of this freedom',[254] it is admitted that freedom to conduct business includes the freedom to exercise an economic or commercial activity, the freedom of contract, and free competition.[255] This freedom protects economic initiative and the ability to participate in the internal market, rather than actual profits earned, while limiting legislative and executive EU actions.[256] It often acts as a counterweight to other fundamental rights.[257] However, the history of Article 16 of the EU Charter shows a much-qualified nature, which allows the state the ability to interfere with this right.[258]

Imposing new burdensome obligations on DSPs would make it more expensive for new players to enter the market. The economic impact of enforcing obligations on DSPs has been highlighted by the CJEU, especially in filtering and monitoring obligations. The CJEU stated that the online monitoring of all works 'would result in a serious

[250]F. Mostert, '"Digital due process": a need for online justice', (2020) 15 *Journal of Intellectual Property Law & Practice*, <doi:10.1093/jiplp/jpaa024>

[251]See European Centre for Algorithmic Transparency <https://algorithmic-transparency.ec.europa.eu/index_en>.

[252]See EU Charter, see n. 116, art 16. On this relatively recent fundamental right and its relation to IP, see G. Ghidini and A. Stazi, 'Freedom to conduct a business, competition and intellectual property', in Geiger (ed.), see n. 121, 410; On potential incompatibility of the DSA with this right, see B. Allgrove, 'The EU's Digital Services Act: are we still free to conduct business?' (*EU Law Live*, 31 May 2021) < https://eulawlive.com/op-ed-the-eus-digital-services-act-are-we-still-free-to-conduct-business-by-ben-allgrove>.

[253]Note, however, that some national constitutions provided for the protection of the freedom to conduct business long before these supranational developments. See eg Italian Constitution of 1947, art 41; Spanish Constitution of 1978, art 38; Croatian Constitution of 1990, art 49; and Slovenian Constitution of 1991, art 74.

[254]Case 426/11 *Mark Alemo-Herron and Others v Parkwood Leisure Ltd*, ECLI:EU:C:2013:82, Opinion of AG Villalón, para. 49.

[255]Ibid., paras 48–52.

[256]Ibid.

[257]Ibid.

[258]See Case 283/11 *Sky Österreich GmbH v Österreichischer Rundfunk*, ECLI:EU:C:2013:28, para. 46; Case T-587/13 *Miriam Schwerdt v Office for Harmonisation in the Internal Market*, ECLI:EU:T:2015:37, para. 55.

infringement of the freedom of the hosting service provider to conduct its business'.[259] The DSPs' freedom of business would be hindered due to the requirement to install costly filtering technologies at their own expense.[260] Further, the CJEU found that enforcing these obligations would infringe on Article 3 of the Enforcement Directive, stating 'procedures and remedies necessary to ensure the enforcement of the intellectual property rights [...] shall not be unnecessarily complicated or costly [and] shall be applied in such a manner as to avoid the creation of barriers to legitimate trade'.[261] In the context of the use of filtering tools, the CJEU Advocate General Opinion in the *YouTube/Cyando* case has examined the requirement 'to check, in a general and abstract manner, all the files which their users intend to publish before they are uploaded in search of any copyright infringement'.[262] The Advocate General emphasised that:

> Requiring online platform operators to check, in a general and abstract manner, all the files which their users intend to publish before they are uploaded in search of any copyright infringement *would introduce a serious risk of undermining these different fundamental rights*. Given the potentially considerable volume of hosted content, it would be impossible to carry out such a check in advance manually and, furthermore, the risk in terms of liability for those operators would be excessive. In practice, the smallest of them would be at risk of not surviving that liability and those with sufficient resources would be forced to carry out general filtering of their users' content, without judicial review, which would result in a substantial risk of 'over-removal' of that content.[263]

To ensure proportional balance of freedom to conduct a business, it is also important to take costs and business dimensions into account.[264] Even though the ECHR presents limited possibilities for the protection of property rights and interests of online platforms, in the *Delfi* follow-up cases, the ECtHR paid attention to the size of the entities involved and measures taken by them. A small blog run by a non-profit association[265] or a small blog run by a local resident and beneficial for the community[266] complied with their obligations employing *ex post* removal of content rather than proactive monitoring.[267] In *GS Media*, the CJEU stressed a distinction between larger for profit professional DSPs and non-for profit unprofessional DSPs, imposing obligations to monitor their networks for infringing links only on the former.[268] Also, the principle of proportionality based on the relationship between costs and business dimensions applies, under Article 17 of the C-DSM Directive, when deciding whether DSPs have fulfilled their obligations under paragraph (4). To do so, the following criteria should be considered '(a) the type, the audience and

[259] *Netlog*, see n. 54, para. 46.

[260] See, in this sense, E. Engstrom and N. Feamster, 'The Limits of Filtering: A Look at the Functionality and Shortcomings of Content Detection Tools' (*Engine*, March 2017), 22 ff (according to which 'filtering tools are prohibitively expensive for many small OSPs" and giving examples of the costs of filtering systems. They conclude that "for smaller OSPs, the cost of these systems would make it significantly harder to attract investors and compete with dominant incumbents. In a survey of investors in the U.S. and EU, a majority of respondents said they would be "uncomfortable investing in businesses that would be required by law to run a technological filter on user uploaded content. [...] Since startups are responsible for virtually all new net job growth in the U.S., the overall economic cost of a mandatory filtering regime for OSPs would likely be significant'). From this economic perspective, any stricter liability regime in the EU might undermine the competitiveness of EU based start-ups. According to P. Samuelson, 'Pushing Back on Stricter Copyright ISP Liability Rules' (2021) 27(2) *Michigan Technology Law Review*, 299, 329, 'there is a reason why US-based Internet platforms have been so much more successful than EU-based firms: The US legal culture is less paternalistic and more hospitable to entrepreneurship and innovation'; Geiger and Jütte, see n.,89 (noting that "overly cost-intensive measures are more likely to restrict Article 16 EUCFR to an extent that cannot be justified with reference to competing FR).

[261] See Directive 2004/48/EC, see n. 72, art 3.

[262] *YouTube/Cyando* AG Opinion, see n. 183, para. 242.

[263] ibid (emphasis added).

[264] EU Member States courts have also ruled on the issue, albeit with different outcomes. See, e.g., French Cour de Cassation, APC et al v. Google, Microsoft, Yahoo!, Bouygues et al, ECLI:FR:CCASS:2017:C100909 (6 July 2017) (finding that an online provider must bear the costs of monitoring); UK Supreme Court, *Cartier v BskyB* [2018] UKSC 28 (finding that access providers should not bear all cost of the blocking injunctions; reversing Court of Appeal decision, [2016] EWCA Civ 658.

[265] *Pihl*, see n. 94, para. 37.

[266] *Jezior v Poland* App. no. 31955/11 (ECtHR, 4 June 2020).

[267] *MTE*, see n. 94, para. 82.

[268] C-160/15 GS *Media BV v Sanoma Media Netherlands BV and Others*, ECLI:EU:C:2016:644, para. 51.

the size of the service and the type of works or other subject matter uploaded by the users of the service; and (b) the availability of suitable and effective means and their cost for service providers'.[269]

In conclusion, the platform liability regime should be thoughtfully designed to balance the fundamental right of DSPs to conduct business with their societal and legal obligations. Special attention must be given to not burden new or smaller players disproportionately, thereby ensuring that regulatory measures don't stifle market participation or free competition. The scope and nature of obligations, particularly those related to filtering and monitoring, must be carefully calibrated to avoid infringement on other fundamental rights and to prevent undue economic burdens. Proportionality should be the watchword, taking into account factors like the platform's size, business model, and type of hosted content. By adhering to these principles, the regime can uphold the EU's internal market principles and align with existing legal frameworks such as Article 3 of the Enforcement Directive and Article 17 of the C-DSM Directive (as interpreted by the CJEU in its *Republic of Poland* decision), thereby creating a balanced and equitable digital services landscape.

3.3 | The necessity of regulating property to secure its social function: inherent limitations of the fundamental right to property

The right to property of IP holders is also vital to take into account when considering intermediary liability and regulation. Actually, the intermediary liability conundrum is mostly about balancing this right against the rights earlier mentioned. In the EU, the fundamental right status of IP is governed by Article 17(2) EU Charter,[270] combined with the interpretative framework of Article 1 Protocol No.1 ECHR, and the ways the courts have enforced these rights determines the balancing at stake.

In Europe, a number of legislative and judicial developments have strengthened fundamental rights protection for IP. Primarily, as mentioned, the EU Charter specifically protects IP rights in Article 17(2). In addition, despite the ECHR not formally recognising IP rights, the ECtHR has interpreted Article 1 Protocol No.1 to include IP rights.[271] This is best observed in the case of *Anheuser-Busch*, which extended the rights afforded in Article 1 to include the registration of trade marks.[272] Again, the ECtHR stated in 2013: '[a]s to the weight afforded to the interest of protecting the copyright-holders, the Court would stress that intellectual property benefits from the protection afforded by Article 1 of Protocol No. 1 to the Convention'.[273] However, in reading these developments, some

[269]Directive 2019/790/EU, see n. 11, Art 17(5).

[270]For further references on the interpretation of art 17 (2), see n. 118. In particular, for a review of the scope of the provision, see Ricolfi, see n. 118, 338–340.

[271]See in the field of copyright: *Akdeniz*, see n. 120; *Neij and Sunde Kolmisoppi*, see n 136; *Ashby Donald and Others v. France*, App. No. 36769/08 (ECtHR, judgment of 10 January 2013); *Balan v Moldova* App. no. 19247/03 (ECtHR, 29 January 2008); *Melnychuk v Ukraine* App. no. 28743/03 (ECtHR, 5 July 2005); *Dima v Romania* App. no. 58472/00 (ECtHR, 26 May 2005). In the field of trade marks: *Paeffgen Gmbh v Germany* App. nos 25,379/04, 21,688/05, 21,722/05 and 21,770/05 (ECtHR, 18 September 2007); *Anheuser-Busch Inc. v Portugal* App. no. 73049/01 (ECtHR, 11 January 2007). In the field of patent law: *Lenzing AG v United Kingdom* App. no. 38817/97 (ECommHR, 9 September 1998); *Smith Kline & French Lab. Ltd v Netherlands* App. no. 12633/87 (ECommHR, 4 October 1990). For a comprehensive overview of the IP-related case law of the ECtHR, see Geiger and Izyumenko, see n. 137, 9; and, more recently, C. Geiger and E. Izyumenko, 'Shaping Intellectual Property Rights Through Human Rights Adjudication: The Example of the European Court of Human Rights', (2020) 46(3) *Mitchell Hamline Law Review* 527.

[272]See Anheuser-Busch, see n. 271. See also M. Ricolfi, 'Trademark and Human Rights', in P. Torremans (ed), *Intellectual Property and Human Rights* (Kluwer Law Int'l 2020), 593–644; K.-D. Beiter, 'The Right to Property and the Protection of Interests in Intellectual Property—A Human Rights Perspective on the European Court of Human Right's Decision in Anheuser-Bush Inc v Portugal', (2008) 39(6) *IIC - International Review of Intellectual Property and Competition Law*, 714, 717.

[273]*Neij and Sunde Kolmisoppi*, see n. 136, para. 10. See also C. Geiger and E. Izyumenko, 'Copyright on the Human Rights Trial: Redefining the Boundaries of Exclusivity through Freedom of Expression', (2014) 45(3) *IIC - International Review of Intellectual Property and Competition Law*, 316. However, case law has also highlighted that when states are balancing two fundamental rights, they are given "a particularly wide" margin of appreciation. See *Neij and Sunde Kolmisoppi*, n. 136, para 11. See also *Akdeniz*, see n. 120, para. 28; *Ashby Donald*, see n. 271, para. 40.

academics have argued that the EU's approach of IP being a fundamental right may result in the overprotection of IP rights and thus fail to strike a balance with other fundamental rights.[274]

The protection granted by the right to property to IP, however, should not be overestimated. The CJEU noted in the case of *Telekabel*: 'there is nothing whatsoever in the wording of Article 17(2) EU Charter to suggest that the right to intellectual property is inviolable and must for that reason be absolutely protected'.[275] Therefore, Article 17(2) could be considered merely as a clarification of Article 17(1), which actually stresses that '[t]he use of property may be regulated by law in so far as is necessary for the general interest'.[276] Likewise, the first paragraph of Article 1 First Protocol ECHR provides for the possibility of restriction of the right 'in the public interest', while the second paragraph allows the state 'to enforce such laws as it deems necessary to control the use of property in accordance with the general interest [...]'.[277] As the preparatory documents of the First Protocol of the ECHR show the new property paradigm was seen as 'relative' in nature compared to the absolute right to own property.[278] In a similar vein, the exclusion of an 'absolutist' conception of IP rights that imbued the preparatory documents of the First Protocol made clear that 'the guarantees laid down in paragraph 1 [of art 17 EU Charter] shall apply as appropriate to intellectual property' and that 'the meaning and scope of Article 17 [EU Charter] are the same as those of the right guaranteed under Article 1 of the First Protocol to the ECHR'.[279]

In this regard, the approach follows Article 27(2) of the UDHR and Article 15(1)(c) of the International Covenant on Economic, Social and Cultural Rights (ICESCR), which implement the 'protection of the moral and material interests resulting from [the authors'] scientific, literary or artistic production'.[280] In this context, the UN Special Rapporteur for cultural rights emphasised that inferring from the wording of these provisions that Article 15(1)(c) recognises the human rights protection of IP rights was 'false and misleading'.[281] Concurring with the UN Special Rapporteur, the UN Committee on Economic, Social and Cultural Rights (CESCR) stressed that there is a clear distinction between IP rights and the fundamental rights protection granted by virtue of Article 15(1)(c) ICESCR.[282] This Article provides limited protection for IP rights but these rights cannot be guaranteed nor are they elevated to the level of fundamental rights altogether for every aspect of their protection.[283] In particular, the social function of property as

[274]See, e.g., for a critique of the approach towards treating IP rights and other fundamental rights 'as if they were of equal rank', A. Peukert, 'The Fundamental Right to (Intellectual) Property and the Discretion of the Legislature', in Geiger (ed), see n. 252, 132; R. Burrell and D. Gangjee, 'Trade Marks and Freedom of Expression: A Call for Caution', (2010) 41(5) *IIC - International Review of Intellectual Property and Competition Law*, 544; C. Angelopoulos, 'Freedom of Expression and Copyright: The Double Balancing Act', (2008) 3 *Intellectual Property Quarterly*, 328. See, however, C. Geiger, 'Fundamental Rights, a Safeguard for the Coherence of Intellectual Property Law?', (2004) 35 *IIC - International Review of Intellectual Property and Competition Law*, 268; C. Geiger, 'Copyright's Fundamental Rights Dimension at EU Level' in Estelle Derclaye (ed.), *Research Handbook on the Future of EU Copyright*, (Edward Elgar 2009), 27; C. Geiger, 'The Social Function of Intellectual Property Rights, or How Ethics Can Influence the Shape and Use of IP Law', in G. Dinwoodie (ed.), *Methods and Perspectives in Intellectual Property* (Edward Elgar 2013), 153, underlining that the property aspects protected at a constitutional level refer to a property *of a special kind*, property with a strong social function, which should therefore not be equated with physical property since it is far more limited in its scope. Under this understanding, IP rights must be construed in a more limited manner than the right to physical property, with constitutional protection of rights over intangibles remaining rather 'weak' in comparison with other rights. For an historical perspective stressing this very point, see also G. Frosio, *Reconciling Copyright with Cumulative Creativity: The Third Paradigm* (Edward Elgar 2018), 161–181.

[275]*Telekabel*, see n. 120, para. 61.

[276]Ibid. See also Ricolfi, see n. 118) 343 (acknowledging that this the "most credited" construction of the norm).

[277]Ibid.

[278]See Council of Europe, 'Preparatory Work on Article 1 of the First Protocol to the European Convention on Human Rights' (13 August 1976) CDH (76) 36, 12 and 16.

[279]Note from the Praesidium, 'Draft Charter of Fundamental Rights of the European Union, Explanations on Article 17 of the EU Charter' (2000), 19–20.

[280]UDHR (n 221) art 27(2); International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966) UNGA Res 2200 A(XXI) (hereafter 'ICESCR'), art 15(1)(c). See in this sense also C. Geiger, 'Building an Ethical Framework for Intellectual Property in the EU: Time to Revise the Charter of Fundamental Rights' in G. Ghidini and V. Falce (eds), *Reforming Intellectual Property Law* (Edward Elgar 2022), (arguing for a revision of Art 17(2) of the Charter to reflect the protection granted by the UDHR and the ICESCR).

[281]UN General Assembly, 'Report of the Special Rapporteur in the field of cultural rights, Farida Shaheed, Copyright Policy and the Right to Science and Culture, Human Rights Council' (2014) A/HRC/28/57, s. 26. On this report, see C. Geiger (ed), *Intellectual Property and Access to Science and Culture: Convergence or Conflict?* (CEIPI/ICTSD 2016) (including a Foreword by the Special Rapporteur).

[282]See CESCR, 'General Comment no. 17 on Article 15(1)(c) of the ICESCR' (12 January 2006) E/C12/GC/17.

[283]ibid. For a detailed analysis of these documents, see C. Geiger, 'Implementing Intellectual Property Provisions in Human Rights Instruments: Towards a New Social Contract for the Protection of Intangibles' in Geiger (ed), see n. 121, 661 ff.

included in all constitutional protections of property implies large room for manoeuvre for legislators to design IP laws taking into account competing fundamental rights and the general interest of society.[284]

Given the foregoing analysis, a balanced platform liability regime should consider a nuanced approach to intellectual property (IP) rights, recognising that these rights, while important, are not absolute. Both EU and ECHR frameworks provide room for regulating the right to property in the public interest. This regulation should be done cautiously to prevent the overprotection of IP rights at the expense of other fundamental rights or societal interests. Legislative measures should heed the limitations inherent in fundamental rights to property as indicated by Article 17(2) of the EU Charter and Article 1 of Protocol No.1 of the ECHR. The regime should also align with international human rights frameworks like the UDHR and ICESCR, which makes a clear distinction between IP rights and fundamental human rights, specifying that only certain creator's interests can benefit from international human rights protection in order to serve as a vehicle to enhance access to science and culture. Importantly, the social function of property should be a key consideration, allowing for legislative flexibility to balance competing rights and the general societal interest.

More generally, Section 3 reveals that the EU's framework for online fundamental rights forms a complex but pragmatic scaffold upon which to construct a comprehensive platform liability regime. It emphasises the need to strike a balanced approach that respects the nuanced interplay among various fundamental rights, including freedom of expression, freedom to conduct business, and intellectual property rights. While the regulatory fabric laid out by EU and ECHR provisions allows for the imposition of obligations on Digital Service Providers (DSPs), these must be carefully calibrated to protect the ecosystem of online platforms—from large, commercial entities to smaller, non-profit players. Importantly, intellectual property rights, although recognised, are not to be overprotected to the point of overshadowing other fundamental rights or societal interests. This leads us to a core set of guiding principles: proportionality, respect for the social function of property, and a balanced recognition of multiple competing fundamental rights. These principles should be at the forefront as legislators and policymakers work to actualise the potential of this complex legal landscape.

4 | TAKING FUNDAMENTAL RIGHTS SERIOUSLY IN THE DSA

Consistency with the fundamental rights framework described above will be tested by the ongoing EU reform actions in the context of the DSA. This pivotal regulation needs to carefully navigate the fundamental rights landscape to prevent unintended negative consequences for both users and DSPs in the Digital Single Market (DSM). This concluding section aims to offer insights into the effective implementation of a platform liability regime that is rooted in the principles of fundamental rights, as framed within the DSA's legislative parameters.

Given the rapid technological development in the past two decades, there has been a widespread agreement that an update of the legal framework for digital services was needed. However, the exact way forward has been the subject of debate.[285] The EP called for legislative proposals to provide 'harmonised requirements for digital service providers to apply effective, coherent, transparent and fair procedures and procedural safeguards to address illegal content in line with national and European law, including via a harmonised notice-and-action procedure'.[286] To this end, the DSA reform has been aiming at (i) clarifying and fully harmonising at EU level rules on liability of DSPs,[287]

[284]See Geiger, see n. 274, 153; C. Geiger, 'Copyright as an Access Right, Securing Cultural Participation through the Protection of Creators' Interests', in R. Giblin and K. Weatherall (eds), *What if we could reimagine copyright?* (ANU) Press 2016), 76 ff; Geiger and Izyumenko, see n. 271, 527 ff.

[285]T. Madiega, 'Reform of the EU liability regime for online intermediaries, Background on the forthcoming digital services act' (European Parliamentary Research Service, May 2020), 19.

[286]EP Resolution on the DSA and FRs, see n. 93, point 25. Proposals have been also made in N. Lomba and T. Evas, *Digital services act: European added value assessment* (European Parliament, October 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654180/EPRS_STU(2020)654180_EN.pdf>, including a series of research papers as annexes: C. Tarín and others, 'Annex I: Quantitative assessment of the European added value of a digital services act'; G. Splinder, 'Annex II: Digital services act: Adapting commercial and civil law rules for commercial entities operating online: Legal assessment'; J. Nordemann and others, 'Annex III: Digital services act: Improving the functioning of the single market'

[287]EP Resolution on the DSA and FRs, see n. 93, point 24.

(ii) while maintaining liability exemptions based on the ECD knowledge-and-take-down principle.[288] (iii) Meanwhile, new unnecessary administrative burdens should be avoided, ensuring that the liability regime does not disadvantage small and medium-sized DSPs or create obstacles to innovation and access to information.[289] (iv) More specifically, from a fundamental rights perspective, the DSA is meant to address the following areas: content management rules; procedural guarantees; algorithmic enforcement and transparency; institutional bodies and decision making.

4.1 | Content management and removal

The DSA incorporates an extensive framework of rules, standards, and procedures for the moderation of content. In practice, illegal content online should be tackled on the basis of the same legal principles and guarantees as illegal content offline.[290] In particular, measures for content moderation introduced by the DSA apparently apply to illegal content only, which is defined as "any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law".[291] Instead, potentially harmful content would not be specifically addressed from a DSA perspective. This represents a constructive approach, given the importance of ensuring that "content that might even be controversial, shocking, or offensive is not prohibited by law simply because it makes certain audiences

[288]The idea of abolishing liability exemptions altogether has been very much residual at least since the late nineties when the first liability exemptions have been enacted after an initial hesitation when the DMCA and §230 CDA were under discussion. See B. Lehman, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights (DIANE Publishing 1995), 114–124 (noting "the best policy is to hold the service provider liable [. . .] Service providers reap rewards for infringing activity. It is difficult to argue that they should not bear the responsibilities."]; see also J. Boyle, Intellectual Property? Two Pasts and One Future, Information Influx International Conference, Amsterdam (July 2–4, 2014), <https://www.youtube.com/watch?v=gFDA-G_VqHo> (discussing how the liability exemptions side finally won the day, in particular by showing the risk of over-enforcement attached to a strict liability system and the potential negative externalities on fundamental rights and technological innovation as this article discusses at length in I.A-C). Liability exemptions have been the principle in the EU since 2000 and the DSA confirmed that regulatory approach without faltering. The DSA reproduces unchanged the liability exemptions provided for by the ECD, in particular the hosting exemption and the principle of no general monitoring obligations. See DSA, see n. 16, Articles 6 and 8. See also EP Resolution on the DSA and FRs, see n. 93, point 24; EP Resolution on the DSA and the Single Market, see n. 94, point 57. Actually, the DSA proposal strengthens even further the ECD knowledge-and-take-down approach by clarifying in the negative the *vexata questio* whether voluntary monitoring makes DSPs ineligible for liability exemption. DSPs shall not be deprived of the protection granted by liability exemptions "solely because they carry out voluntary own-initiative investigations or other activities aimed at detecting, identifying and removing, or disabling of access to, illegal content, or take the necessary measures to comply with the requirements of Union law, including those set out in this Regulation". See DSA, see n. 16, art 6. In fact, multiple alternative positions have been emerging among scholars prior to the publication of the DSA proposal, in particular aiming at narrowing down the scope of the exemption by crafting some additional specific exceptions. See, (1) supporting the preservation of "conditional immunity from liability for third-party content", A. de Streel and M. Husovec, "The e-commerce Directive as the cornerstone of the Internal Market, Assessment and options for reform', Study for the committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies (European Parliament, May 2020) (hereafter 'Study on the e-commerce Directive'), 48; Article 19's Recommendations for the EU Digital Services Act (*Article 19*, 21 April 2020), <https://www.article19.org/wp-content/uploads/2020/04/ARTICLE-19s-Recommendations-for-the-EU-Digital-Services-Act-FINAL.pdf> (hereafter 'Article 19's Recommendations'), Recommendations 2; (2) proposing readjustment and fine-tuning of the safe harbour principle, H. Schulte-Nölke and others, 'The legal framework for e-commerce in the Internal Market, State of play, remaining obstacles to the free movement of digital services and ways to improve the current situation', Study for the committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies (European Parliament, May 2020), 37; (3) arguing that DSPs should face a duty to prevent further infringements of the same kind, J. Nordemann, 'Internal Market for digital services: Responsibilities and duties of care of providers of digital services, Study for the European Parliament Committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies' (European Parliament, 2020), 42; (4) in favour of extension of safe harbours to cover to 'active' providers, G. Sartor, 'New aspects and challenges in consumer protection, Digital services and artificial intelligence', Study for the committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies (European Parliament, April 2020), 8; C. Schmonn, 'Our EU Policy Principles: Platform Liability' (*EFF*, 9 July 2020), <https://www.eff.org/deeplinks/2020/07/effs-eu-policy-principles-platform-liability-and-monitoring>; (5) incorporating the 'Good Samaritan' principle in the DSA, J. Barata, 'Positive Intent Protections: Incorporating a Good Samaritan principle in the EU Digital Services Act' (*Center for Democracy & Technology*, 29 July 2020) <https://cdt.org/insights/positive-intent-protections-incorporating-a-good-samaritan-principle-in-the-eu-digital-services-act/>.

[289]See EP Resolution on the DSA and FRs, see n. 93, point 18. See also Article 19's Recommendations, see n. 288, Recommendations 7 (recommending that measures should be designed to take into consideration the degree of market power of internet intermediaries).

[290]See DSA, see n. 16, art 3(h) and Recital 12 (qualifying further the notion as a "concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that the applicable rules render illegal in view of the fact that it relates to illegal activities"); EP Resolution on the DSA and FRs, see n. 93, point 2.

[291]EP Resolution on the DSA and commercial and civil rules, see n. 95, point 3; EP Resolution on the DSA and FRs, see n. 93, point 5.

uncomfortable'.[292] The DSA also introduces the concept of "manifestly illegal content", though its definition is somewhat circular. According to a Recital in the Regulation, content is considered "manifestly illegal" if "it is evident to a layperson, without any substantive analysis, that the content is illegal".[293] This category is tied to a specific obligation for online platforms: they are required to temporarily suspend their services, after issuing a prior warning, to users who repeatedly post such manifestly illegal content.[294] Within this framework, the DSA could have opted for a more nuanced strategy by employing different regulatory approaches for distinct categories of content, namely manifestly illegal, simply illegal, and other types of content.[295] We will elaborate on this shortly. Before delving further, it's important to highlight that alongside its definition of "illegal content", the DSA could have benefitted from offering a specific definition for "manifestly illegal content". A well-articulated distinction between illegal and merely harmful content would have also added clarity to the regulatory framework.[296] Along with apology of acts constituting an offence against human dignity, war crimes, crimes against humanity, human trafficking, incitement to or apology of violence, acts of terrorism and child abuse content, manifestly illegal content could include manifestly IP infringing content for which no equity-based assessment is needed.[297] In this latest regard, any content that might encompass a privileged use[298] or whose protected status could be otherwise questioned should never be considered"manifestly illegal". For the purpose of future fine-tuning of the reform,[299] clearer and more stringent definitions should be established for all types of manifestly illegal content. Such categorisation should be subject to strict interpretation to ensure clarity and precision in the regulation's application.

In accordance with the DSA, while illegal content should be removed swiftly and consistently,[300] such removals should be in line with fundamental rights standards.[301] Nonetheless, the DSA could have been more explicit in stipulating that streamlined removal processes, including the use of automated tools, should be restricted to content that is either manifestly illegal or has been declared illegal by an independent authority, whether judicial or quasi-judicial.[302] This is in line with the fundamental rights limitations discussed in Section 2, which require such restrictions

[292]R. Wingfield, 'The Digital Services Act and Online Content Regulation: A slippery slope for human rights?' (*Medium*, *The GNI Blog*, 15 July 2020) <https://medium.com/global-network-initiative-collection/the-digital-services-act-and-online-content-regulation-a-slippery-slope-for-human-rights-eb3454e4285d>.

[293]See DSA, see n. 16, Recital 63.

[294]Ibid., Article 23.

[295]Cf. Wingfield, see n. 296.

[296]See EP Resolution on the DSA and commercial and civil rules, see n. 95, Annex to the Resolution, 12; EP Resolution on the DSA and the Single Market, see n. 94, point 47 (noting, in particular, that illegal content, punishable acts and illegally shared content should be distinguished from harmful, but not necessarily illegal, content such as disinformation). See also, in support of the distinction, Wingfield, see n. 292; M. Land, 'Remedy and Enforcement in the Digital Services Act' (*Medium*, *The GNI Blog*, 4 August 2020) <https://medium.com/global-network-initiative-collection/remedy-and-enforcement-in-the-digital-services-act-by-professor-molly-land-a37b31b61ed5>; Article 19's Recommendations (n 288) Recommendation 4.

[297]See, for discussion on the definition of manifestly illegal content, EP Resolution on the DSA and FRs, n. 93, point 33; EP Resolution on the DSA and commercial and civil rules, n. 95, Annex to the Resolution, 19, 25. Moreover, EP Resolution on the DSA and commercial and civil rules, n. 95, suggests defining it as content which 'unmistakably and without requiring in-depth examination [is] in breach of legal provisions regulating the legality of content on the internet'.

[298]A good example for such a privileged use in the field of copyright are exceptions and limitations which have been qualified as users' right and need to be safeguarded from a fundamental rights perspective (see *supra*).

[299]See DSA, see n. 16, Recital 102 (noting that in the context of the potential promotion of voluntary standards to facilitate the effective and consistent application of the obligations in the Regulation, such "standards could distinguish between different types of illegal content

[300]See DSA, see n. 16, Recital 22 and, on the speed and quality of processing of notices, Recital 87; EP Resolution on the DSA and FRs, see n. 93, point 3.

[301]See DSA, see n. 16, Recital 22, 53–54, and Article 17 (specifically noting at Recital 54 that information on reasons of a removal decision and available redress should be given in view of the negative effect that the decision might have, especially as regards the exercise of the fundamental right of freedom of expression). See also A. Peukert, M. Husovec, M. Kretschmer, P. Mezei and J. P. Quintais, 'European Copyright Society – Comment on Copyright and the Digital Services Act Proposal', (2022) 53(3) *IIC - International Review of Intellectual Property and Competition Law*, 358, 369; J. P. Quintais, C. Katzenbach, S. B. Schwemmer, D. Dergacheva, T. Riis, P. Mezei and I. Harkai, 'Copyright Content Moderation in the EU: Conclusions and Recommendations', in *reCreating Europe Report* (2022), 25–27 <https://ssrn.com/abstract=4403423>.

[302]According to the DSA, orders issued by a judicial or administrative authority to act against illegal content must meet a set of conditions meant to safeguard rights of the affected parties. The orders should contain: (i) a statement of reasons explaining why the information is illegal content, with reference to specific legal provisions infringed; (ii) exact uniform resource locators and any information enabling the identification of the illegal content; (iii) information about redress available to the DSPs and their users providing the content. See DSA, see n. 16, Article 9. Similar safeguards would also apply to orders against DSPs to provide a specific item of information about individual recipients of digital services. ibid, Article 10 (1–2).

to be qualified and carefully delineated.[303] Instead, should any doubts exist as to the content's 'illegal' nature, such content should be subject to human review and not be removed without further investigation, either carried out internally by the DSPs or much more preferably run by external, independent entities.[304] Depending on the complexity of the review, in cases especially doubtful, further scrutiny might be required. For example, DSPs might be required to set up a moderation system so that content flagged by human reviewers go through a second round of review, this time by panels of more qualified reviewers. However, to mitigate the complex issue of private entities making decisions that affect the fundamental rights of users, an additional layer of review could be beneficial for borderline cases. Ideally, this should be conducted by an entity that operates independently from the DSPs. For instance, a specialised EU entity could be established to scrutinise and decide upon intricate content moderation scenarios. This entity's intervention in the moderation cycle would further guarantee users' fundamental rights and provide legal certainty for content moderation.[305] Finally, requiring platforms to remove manifestly illegal content within unduly short timeframes might be problematic,[306] and should be avoided or limited to illegal content that might cause imminent harm, such as illegal hate speech, child pornography, revenge porn, incitation to violence or terrorist content.[307]

As mentioned already, legal content should not be subject to any legal removal or blocking obligations.[308] Disinformation would be a sensitive category that might fall within the notion of legal but harmful content. While the focus of all DSA's content moderation obligations is on "illegal content", the final version of the DSA does make also a few scattered references to tackling online disinformation and other societal risks.[309] Nonetheless, these concerns appear to be absent from the actionable sections of the Regulation, where the term "disinformation" never appears. While the dispositive part of the DSA makes explicit reference only to "illegal content", avoiding mentions of disinformation or other societal risks, the legislative intent seems clearly aimed at sparing platforms from explicit obligations to police such issues. In this context, the jurisprudence of the ECHR that was mentioned earlier might serve as a guidance for distinguishing between harmful and illegal disinformation. Disinformation should be blocked and removed, as illegal content, only in those instances when the ECtHR would deploy the extreme tool of Article 17 ECHR - abuse of rights – for addressing unfactual information, including cases such as Holocaust denial, and perhaps more generally misinformation denying crimes against humanity if they are established historical facts.[310]

Still, the wording in Article 34(2) could potentially mandating platforms to address and filter out disinformation. This Article calls for a systemic risk assessment that includes an analysis of "whether and how the risks […] are influenced by intentional manipulation of their service, including by inauthentic use or automated exploitation of the service, as well as the amplification and potentially rapid and wide dissemination of illegal content and of *information that is incompatible with their terms and conditions*."[311] The explanatory Recital for this provision indicates that such risks could stem from activities like the establishment of fake accounts, deployment of bots, or deceptive utilisation

[303]Cf. EP Resolution on the DSA and the Single Market, see n. 94, point 33. Consideration, however, must be also given to possible technical limitations to perform the automated filtering requested. In the aftermath of the DSA, this could be monitored by an independent authority to be set up in order to secure that the obligation is feasible and does not lead to significant overblocking of legitimate content (see infra).

[304]See EP Resolution on the DSA and the Single Market, see n. 94, point 50.

[305]In order to enhance legal certainty and to safeguard the DSP's freedom to conduct a business, this entity could also be entrusted with developing relevant guidelines or principles agreed upon by the relevant stakeholders. Anyhow, the future scope and mission of such an EU agency cannot be duly developed here and would need further detailed examination in the future. For a detailed proposal to set up an independent EU institution to i.e. monitor the copyright content moderation process set up by Article 17 CDSM, see C. Geiger and N. Mangal, 'Regulating Creativity Online: Proposal for an EU Copyright Institution', (2022) 71(10) *GRUR International*, 933–951 <https://ssrn.com/abstract=4107644>.

[306]See, in this sense, Article 19's Recommendations (n 288) Recommendation 5. In this respect, it is illustrative the French Constitutional Court's declaration of unconstitutionality of the provision of the French draft law 'Proposition de loi contre les contenus haineux sur Internet' (known as 'loi Avia') that imposed the obligation upon DSPs to remove 'manifestly illegal' content within 24 hours following a notification. See Commentaire, Décision n° 2020–801 DC du 18 juin 2020 'Loi visant à lutter contre les contenus haineux sur internet'. See also Article 19, 'France: Analysis of draft hate speech bill' (*Article 19*, 3 July 2019) <https://www.article19.org/resources/france-analysis-of-draft-hate-speech-bill/>.

[307]See DSA, see n. 16, Recital 87

[308]See EP Resolution on the DSA and FRs, see n. 93, point 33.

[309]See DSA, see n. 16, Recital 3, 9, 69, 83–84, 88, 95, 104, 108.

[310]See Section 3.2.1.1 and n. 167).

[311]See DSA, see n. 16, Article 34(2).

of a service, "which may lead to the rapid and widespread dissemination to the public of information that is illegal content or incompatible with an online platform's or online search engine's terms and conditions and that *contributes to disinformation campaigns*."[312] Nevertheless, this language could encourage platforms to moderate content contributing to disinformation campaigns, even when such content does not meet the strict definition of "illegal content". Failing to do so may potentially trigger the need for risk mitigation strategies. Therefore, this wording in Article 34(2) could prompt platforms to revise their Terms of Conditions to prohibit such content. However, this becomes problematic as the DSA doesn't clearly define what constitutes 'disinformation'—a term inherently elusive due to its changing nature. This absence of a standardised definition could lead to a fragmented landscape of private ordering, which could, in turn, risk overly broad censorship in an effort to mitigate systemic risks.

In order to minimise removal and blocking of legal content on the basis of Terms of Service (ToS), guidelines should be agreed upon to increase transparency rules for content moderation policy,[313] while prohibiting any discriminatory content moderation practices.[314] In this context, the DSA mandates that intermediary service providers must conduct themselves in a "diligent, objective and proportionate" manner when enforcing restrictions outlined in their Terms of Service.[315] This is to be done with careful consideration for the rights and legitimate interests of all parties concerned, including safeguarding the service recipients' fundamental freedoms such as "the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter".[316] As further safeguard against removal and blocking of legal content, even though ToS are binding on the parties, take-down orders from competent authorities, including courts, must always be based on legislative provisions, rather than private ToS.[317] In any event, if DSPs restrict legal content of their users on their own initiative, the possibility of content labelling instead of take-downs should be preferred.[318] Removal of content should not be the only possible remedy, but rather the DSA should have encouraged more proportional responses from platforms with a range of remedial actions available, including greater user choice regarding the content they see, DSPs' flagging of inappropriate/harmful content, users' flagging or other counter-speech, such as like or dislike.[319]

Finally, the DSA clarifies that DSPs voluntary own-initiative investigations and other activities aimed at detecting and removing illegal content or at being otherwise compliant with EU law do not deprive DSPs of any of the liability exemptions ("mere conduit", caching, and hosting), if they are carried out in good faith and in a diligent manner.[320] This provision seems to authoritatively resolve in the negative the enduring open question whether voluntary content moderation measures might serve to construe DSPs as active rather than passive or neutral.[321] On one side, this provision is meant to promote voluntary and proactive filtering further by confirming that such actions do not deprive DSPs from immunity. Entitlement to immunity would be only based on the active/passive nature of the DSPs business model as such rather than any enforcement initiative that DSPs can carry out in order to comply with EU law. However, on the other side, this clarification might also produce negative externalities over freedom of expression, leading to overenforcement, given that DSPs will avoid liability when removing content, while gaining now legal certainty of remaining passive service providers, thus enjoying immunities, if that is the case. Apparently, the provision might have, in this sense, opposite effects to a "Good Samaritan" clause in the style of 47 U.S.C. § 230, to which Article 7 of the DSA has been inappropriately compared by some.[322] The clarification in Article 7 of the DSA, however,

[312]ibid, Recital 84 (emphasis added).
[313]See EP Resolution on the DSA and FRs, see n. 93, point 34; EP Resolution on the DSA and the Single Market, see n. 94, point 35.
[314]See EP Resolution on the DSA and commercial and civil rules, see n. 95, point 6.
[315]See DSA, see n. 16, Article 14
[316]ibid
[317]Cf. EP Resolution on the DSA and FRs, see n. 93, point 32.
[318]ibid, point 4.
[319]See, e.g., M. Land and R. Hamilton, 'Beyond Takedown: Expanding the Toolkit for Responding to Online Hate', in Predrag Dojcinovic (ed), *Propaganda, War Crimes Trials and International Law: From Cognition to Criminality* (Routledge 2020), 143.
[320]See DSA, see n. 16, Article 6 and Recital 25.
[321]See n. 67.
[322]See A. Kuczerawy, "The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act", *Verfassungblog*, 12 January 2021 <https://verfassungsblog.de/good-samaritan-dsa> (noting, *inter alia*, that the practical effects that Article 6 might have in terms of overenforcement would be at odds with the overall emphasis on the preservation of fundamental rights, including freedom of expression, that characterises the DSA Proposal).

was due and in line with a logical construction of the ECD, which allows both general and specific voluntary enforcement measures that might imply monitoring and filtering, even in an automated form. In fact, it would be impractical and counter-intuitive to disincentivise good faith and diligent voluntary content moderation, for fear of possible over-blocking, by maintaining in place uncertainties in the construction of certain legal principles. Instead, rather than disincentivising diligent content moderation, voluntary measures must be only applied according to the safeguard that we discuss in this and the following sections and in light of the overall principle in Recital 22 of the DSA that "removal or disabling of access should be undertaken in the observance of [...] the right of freedom of expression".[323]

4.2 | Procedural guarantees (notice-and-action and complaint mechanisms)

The DSA regulates and institutionalises content moderation practices via the introduction of procedural guarantees that comply with the broad framework of fundamental rights,[324] such as the protection of privacy, non-discrimination and dignity, freedom of expression.[325] On one side, the DSA associates effective protection of user rights with the possibility for users to obtain more information about content moderation practices, including transparency of the content removal process and human oversight.[326] Users should be granted more influence and control regarding the content they see and have the option to opt out from any content curation other than chronological order.[327] Moreover, recommendation systems should be 'user-friendly and subject to full transparency'.[328]

On the other side, in the context of content removal,[329] procedural guarantees for notice, counter notice and complaint procedures must be ensured, including transparency of the process and human oversight, in order 'to allow content owners and uploaders to defend their rights adequately and in a timely manner, and to ensure that removal or blocking decisions are legal, accurate, well-founded, protect users and respect fundamental rights'.[330] Specifically, the DSA lays out a notice-and-action framework that incorporates safeguards to uphold fundamental rights, offering a structured procedure for dealing with content issues.[331] In order to do so, the DSA is meant to provide guidance regarding: (i) the right to issue a notice and the form of notices[332]; (ii) procedural safeguard for

[323]DSA, see n. 16, Recital 22.

[324]ibid, art 14(4) (stating that in applying and enforcing any restrictions to the use of their services, DSPs shall act with due regard to the fundamental rights of the users).

[325]Cf. Spindler, see n. 286, 193, 203–208 (discussing content curation and fundamental rights in the DSA); M. Senftleben, J. P. Quintais and A. Meiring, see n. 196, 8–10, 21–23, 56–61.

[326]ibid, Art. 14(1) (providing that DSPs' terms and conditions must include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review'). In addition, the Commission will maintain and publish a Transparency Database, which will collect and analyse statements of reasons, enabling the study of the prevalence of legal threats. See ibid, Recital 66 and Article 24(5); DSA Transparency Database <https://transparency.dsa.ec.europa.eu>. See also, on this matter, J. P. Quintais, N. Appelman and R. Ó Fathaigh, 'Using Terms and Conditions to apply Fundamental Rights to Content Moderation', (2023) 24(5) *German Law Journal* 881, 895–909.

[327]Cf. EP Resolution on the DSA and commercial and civil law rules, see n. 95, point 28; EP Resolution on the DSA and the Single Market, see n. 94, Annex to the Resolution, 28.

[328]Cf. EP Resolution on the DSA and FRs, see n. 93, point 35.

[329]See Spindler, n. 286, 193–203 (discussing content moderation and control); J.-P. Schneider, K. Siegrist and S. Oles, 'Collaborative Governance of the EU Digital Single Market established by the Digital Services Act', (2023) University of Luxembourg Law Research Paper No. 2023–09, 28–32 <https://ssrn.com/abstract=4561010>.

[330]EP Resolution on the DSA and the Single Market, see n. 94, points 11 and 29. See also Spindler, see n. 286, 209–212 (discussing notice procedures)). As per the adequacy of the notice procedure to fundamental rights, the DSA categorises as a risk, subject to systemic risk assessment and mitigating measures, the misuse of very large online platforms" service "through the submission of abusive notices or other methods for silencing speech or hampering competition". DSA, see n. 16, Recital 81.

[331]See DSA, see n. 16, Recital 41, 52 (including (i) the right to freedom of expression and information, (ii) the right to respect for private and family life, (iii) the right to protection of personal data, (iv) the right to non-discrimination and (v) the right to an effective remedy of the recipients of the service, (vi) the freedom to conduct business, including the freedom of contract, of service providers, (vii) as well as the right to human dignity, (viii) the rights of the child, (ix) the right to protection of property, including intellectual property, and (x) the right to non-discrimination of parties affected by illegal content).

[332]ibid, Article 16(1) (stating that the submission mechanism should be user-friendly and by electronic means), (2) (clarifying that notices should be sufficiently precise and adequately substantiated and defining the elements that a notice should include) and (3) (noting that if the requested formalities of the notice are fulfilled, the notice "shall be considered to give rise to actual knowledge"). See also EP Resolution on the DSA and the Single Market, see n. 94, Annex to the Resolution, 30–31.

processing notices and for final decision-making,[333] with a special regime that might be applied to trusted flaggers[334]; (ii) safeguards against the abuse of the system allowing to sanction parties that systematically and repeatedly submit wrongful notices (or manifestly illegal content)[335]; (iii) transparency reports[336]; (iv) access to internal complaint mechanisms that should be transparent, effective, fair and expeditious[337]; as well as (v) the possibility to resort to out-of-court dispute settlement mechanisms and judicial redress.[338] In this context, while the reform does provide mechanisms for the rapid and easy reinstatement of wrongfully removed content or deactivated accounts,[339] it falls short in offering additional guidelines that could better safeguard fundamental rights. Specifically, content that has been the subject of a notice should remain accessible, barring content that is manifestly illegal, until a legality assessment is complete or unless there is a standing judicial or administrative order mandating its removal.[340] Meanwhile, in order to avoid overblocking and preserve freedom to conduct a business, DSPs should be exempt from liability for opting to retain content until its legal status is definitively assessed, and the limited liability regime should be applicable irrespective of the assessment's final determination.

Impartial, transparent, and quick resolution of disputes between users and online platforms requires either modernising and strengthening the existing mechanisms or the establishment of new independent dispute settlement bodies.[341] In this regard, Article 18 of the DSA outlines a framework for certifying out-of-court dispute settlement bodies. These bodies would be accredited by the Digital Service Coordinator—a new entity established by the DSA–of the body's Member State of establishment, provided they meet specific criteria, such as impartiality, independence, expertise, technological capability, cost-efficiency and procedural fairness.[342] Once certified, these bodies, staffed with independent legal experts, could either be established by or receive supported from Member States,[343] and be partly founded by DSPs through a specific tax mechanism. When internal complaints are resolved, the complainants should be informed of the option of out-of-court dispute settlement.[344] The Commission should maintain and publicise a list of certified bodies on a dedicated website and DSPs should inform complainants accordingly.[345] Of course, individuals should retain the option for further judicial redress, irrespective of utilising these dispute resolution bodies.[346]

[333]ibid, Article 16(6) (mentioning that the processing and decision-making should happen in a timely, diligent, and objective manner). According to Article 17 of the DSA, the hosting provider must inform the user of the content removal or blocking and provide "a clear and specific statement of reasons of that decision", including a number of information listed in Article 17(2). In addition, decisions and statement of reasons must be published in a publicly accessible database maintained by the Commission. ibid, Article 17(4).

[334]ibid, Article 22 (requiring DSPs to promptly handle notices from "trusted flaggers"; these trusted flaggers gain their status from the Digital Service Coordinator in their home Member State, based on criteria such as domain expertise, collective interest representation, independence from DSPs, and procedural fairness and efficiency.).

[335]ibid, Recital 57, Article 16(2)(d) and Article 23(1)–(2) (noting that, for both notices and illegal content, suspension should occur for a reasonable period of time and after having issued a prior warning). In particular, the status of "trusted flagger" can be revoked, following an investigation, if, *inter alia*, the trusted flagger "submitted a significant number of insufficiently precise or inadequately substantiated notices". ibid, Article 22(5–6).

[336]ibid, Articles 15, 24, and 42 (setting transparency reporting obligations respectively for providers of intermediary services, providers of online platforms, and VLOPs and VLOSEs).

[337]Ibid., Article 20 (providing that DSPs must make available an online, free-of-charge, internal complaint-handling mechanism for at least six months following decisions to (a) remove or disable access to the information; (b) suspend or terminate the provision of the service, in whole or in part, to the recipients; (c) suspend or terminate the recipients" account).

[338]Ibid., Article 21. See also EP Resolution on the DSA and the Single Market, see n. 94, Annex to the Resolution, points 53, 54.

[339]Ibid, Article 16(6) (providing that complaints must be handled in "a timely, diligent, non-arbitrary and objective manner); ibid, Article 20(4) (if it is the case, decisions must be reversed "without undue delay" as a result of the internal complaint-handling system).

[340]Cf. EP Resolution on the DSA and commercial and civil rules, (n 95) Annex to the Resolution, 25.

[341]See EP Resolution on the DSA and the Single Market, see n. 94, point 89; EP Resolution on the DSA and commercial and civil law rules, see n. 95, Annex to the Resolution, 11. See also Spindler, see n. 286, 213–216 (discussing dispute settlement)

[342]See DSA, see n. 16, Article 21(2).

[343]Ibid., Article 21(4).

[344]Ibid., art 20(5).

[345]Ibid., Article 21(5).

[346]See EP Resolution on the DSA and commercial and civil law rules, see n. 95, Annex to the Resolution, 11, 19, 25–26. For an assessment of the procedural approach through the lens of access to justice, see, P. Ortolani 'If You Build It, They Will Come: The DSA's "Procedure Before Substance" Approach' (*Verfassungsblog*, 7 November 2022) <https://verfassungsblog.de/dsa-build-it>.

4.3 | Algorithmic enforcement and transparency

Unlike Article 17 of the C-DSM Directive,[347] the DSA does not contain any obligation for hosting service providers or other technical intermediaries to use automated tools in content moderation. This decision comes in the wake of a debate that occurred during the approval of the DSA, pointing at the opaqueness of algorithmic tools.[348] In accordance with the *Glawischnig-Piesczek* ruling, DSPs could potentially be required 'to execute periodic searches for distinct pieces of content that a court had already declared unlawful'.[349] However, while the exact method of compliance with DSA obligations may be chosen by the platforms, any measure provided for by the DSA should not constitute, "either de jure, nor de facto, [...] a monitoring obligation with respect to obligations of a general nature".[350] As Senftleben and Angelopoulos also argue, to the extent that filtering would fail to provide adequate protection to fundamental rights, it cannot be imposed on DSPs.[351]

Instead, the DSA includes provision to promote transparency, non-discrimination[352] as well as fundamental rights compliance[353] of algorithmic decision-making when deployed by platforms.[354] Measures to ensure non-discrimination and transparency of algorithms and data sets should be the cornerstone of an effective DSA reform,[355] while the use of automated tools should be 'proportionate, covering only justified cases'.[356]

Firstly, platforms are obligated to disclose the employment of automated tools and algorithmic decision-making processes in content moderation. This information must be included in three key areas: (i) the Terms of Service agreements,[357] (ii) the notification sent to the entity that initially flagged the content,[358] and (iii) the statement of reasons provided alongside decisions to remove or block content.[359] In this context, the DSA might have benefitted from a more nuanced approach by mandating that platforms flag at what stage algorithmic tools are deployed in the decision-making process.[360] Additionally, platforms should be obligated to maintain transparency concerning data sets used for training the algorithms.[361] Also, the logic underpinning automated decisions should be clearly articulated,[362]

[347]See Directive 2019/790/EU, see n. 11, Article 17

[348]See EP Resolution on the DSA and FRs, see n. 93, point 13. See also EP Resolution on the DSA and the Single Market, see n. 94, point 45; EP Resolution on the DSA and commercial and civil law rules, see n. 95, point 12.

[349]See EP Resolution on the DSA and FRs, see n. 93, point 27.

[350]See DSA, see n. 16, Recital 30. See also Article 8; EP Resolution on the DSA and FRs, see n. 93, point 28.

[351]Senftleben and Angelopoulos, see n. 56. See also Senftleben et al., see n. 196, 6–10.

[352]See EP Resolution on the DSA and FRs, see n. 93, point 21.

[353]EP Resolution on the DSA and the Single Market, see n. 94, point 39. See also Spindler, see n. 286, 193–203 (discussing content moderation, in particular via algorithmic tools); A. Peukert and others, 'European Copyright Society: Comment on Copyright and the Digital Services Act Proposal', (2022) 53 IIC 369 <https://ssrn.com/abstract=4016208>

[354]It is in this context that the European Centre for Algorithmic Transparency (ECAT) emerges as an indispensable tool for advancing algorithmic transparency. Situated within the architecture of the European Commission and hosted by the Joint Research Centre (JRC), ECAT operates in close collaboration with the DG CONNECT. The ECAT serves a multi-dimensional role by providing scientific and technical expertise, thereby augmenting the European Commission's exclusive supervisory and enforcement capacities over systemic obligations laid down for VLOPs and VLOSEs by the DSA. Its involvement signifies a concerted effort to comprehend the nuanced ways in which algorithms shape content visibility and promotion, along with their broader societal and ethical repercussions. To this end, experts at the ECAT engage in interdisciplinary dialogue with industry stakeholders, academicians and civil society groups. Their collective endeavours aim to deconstruct algorithmic operations, assess associated risks, and develop transparent algorithmic approaches aligned with best practices. See ECAT <https://algorithmic-transparency.ec.europa.eu/index_en>.

[355]Transparency obligations should also apply to users profiles' content curation.

[356]See EP Resolution on the DSA and commercial and civil rules, see n. 95, point 'H'.

[357]DSA, see n. 16, Article 14(1)

[358]ibid, Recital 54, Article 16(6).

[359]Ibid., Article 17(3)(c).

[360]See S. Windwekr and C. Schmonn, 'Our EU Policy Principles: Procedural Justice' (*EFF*, 27 July 2020) <https://www.eff.org/deeplinks/2020/07/our-eu-policy-principles-procedural-justice>.

[361]See EP Resolution on the DSA and commercial and civil law rules, see n. 95, point 13. More safeguards in this context might be soon introduced by the AI Act Proposal, see n. 30.

[362]The DSA provides that either the Digital Service Coordinator of the Member State of establishment or of the Commission can ask VLOP and VLOSE to explain the design, the logic, the functioning and the testing of their algorithmic systems, including their recommender systems. Also, the logic underpinning automated decisions should be clearly articulated, and platforms should offer specific guidance on how users can challenge these decisions, given potential black-box challenges hurdles involved. Article 40(3).

and platforms should offer specific guidance on how users can challenge these decisions, given the potential black-box hurdles involved in contesting automated decisions.[363]

Secondly, when automated methods are utilised in internal complaint-handling systems, a human review process must be in place to ensure the accuracy and fairness of outcomes.[364] This serves as an essential safeguard against potential errors or biases that could arise from automated decision-making. In its practical implementation, the DSA should adhere to the 'human-in-command' principle, ensuring that all decision-making processes fall under human oversight. This principle mandates not just the ability to monitor the AI system's overall activities and impacts, but also the discretion to determine the circumstances and manner in which the system is employed.[365] Ideally, human review should be conducted by an independent legal expert with specialised competence to ensure a thorough and accurate evaluation. Many content filtering decisions raise intricate legal questions that can be challenging for an in-house reviewer to resolve adequately. The value of human review is fully realised only when the reviewer has the ability to contextualise and assess complex situations in relation to their legality. Take copyright law as an example: the reviewer must have the expertise to assess the legality of a use of content with respect to both EU law and the specific laws of 27 Member States, given that copyright exceptions and limitations are not harmonised. Given the absence of explicit provisions in the DSA regarding this issue, the regulatory oversight mechanisms established by the DSA ought to offer comprehensive legal guidelines for human reviewers. Additionally, these oversight mechanisms should consider introducing frameworks that enable independent review of platform decisions. It's important to acknowledge the impracticality for platforms to employ an extensive team of legal experts to cover every category of content requiring moderation. In this context, perhaps the focus on specialised legal expertise could be most effectively applied within the framework of out-of-court dispute settlements as laid out in Article 21 of the DSA. Here, specialised legal professionals could be engaged to ensure that complex legal considerations are adequately addressed, thereby safeguarding the integrity of the review process and the fundamental rights of all parties involved. The absence of explicit obligations requiring specialised expertise at some stage of the content moderation process represents a suboptimal choice. This oversight should be addressed either during the implementation phase or in future amendments to the reform.

Thirdly, the DSA mandates a comprehensive risk assessment related to the design of algorithmic systems for VLOPs and VLOSEs. This is coupled with an obligation to implement mitigating measures, particularly focusing on how these platforms' services may influence the exercise of fundamental rights,[366] adapting the design, features or functioning of their services, including their online interfaces,[367] adapting content moderation processes, as well as adapting any relevant decision-making processes and dedicated resources for content moderation.

Fourthly, the DSA imposes upon DSPs an obligation to submit annual transparency reports, which should also be published on a publicly accessible database.[368] These reports must detail any use made of automated means for the purpose of content moderation, including (i) a qualitative description, (ii) a specification of the precise purposes, (iii) indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and (iv) any safeguards applied.[369]

[363]See Windwekr and Schmonn, see n. 360. See also DSA, see n. 16, Article 16(5) (merely mandating that the provider must provide information on the possibilities for redress in respect of the decision).

[364]DSA, see n. 16, Article 20(6) and Recital 58.

[365]See EP Resolution on the DSA and the Single Market, see n. 94, point 41 and Annex to the Resolution, 28. See also High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines For Trustworthy AI' (European Commission, 8 April 2019) 15 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419>.

[366]DSA, see n. 16, Recital 81.

[367]Ibid., Article 35.

[368]See, for further information on the nature of these reports, ibid, Article 15 and 24 (with obligations applying respectively to intermediary services and online platforms). See also EP Resolution on the DSA and commercial and civil rules, see n. 95, Annex to the Resolution: Detailed Recommendations as to the Content of the Proposal Requested, 28. Such report should include (i) information on notices processed by the content hosting platform, such as the total number of notices received, for which types of content and the action taken accordingly; (ii) information regarding those who submitted notices; and, (iii) information on counter-notices and appeals etc.).

[369]DSA, see n. 16, Article 15.

Fifthly, to bolster accountability, providers of VLOPs and VLOSEs are subject to independent audits, evaluating their adherence to the DSA.[370] These audits should include thorough examinations of algorithmic systems.[371] To facilitate effective auditing, such providers must offer full cooperation, including granting auditors access to pertinent data and premises.

Finally, as an essential area for future reform, the DSA currently falls short in adequately defining accountability, liability, and redress mechanisms for potential harm stemming from the utilisation of AI applications, automated decision-making, and machine learning tools.[372] Ideally, a more comprehensive framework should be instituted to govern these technologies, delineating specific responsibilities and liabilities for service providers.[373] Moreover, clear channels for redress should be made available for individuals adversely affected by automated decisions. This gap in the DSA necessitates attention in the ongoing discussions for regulatory improvement.

4.4 | Institutional bodies and decision making

The European Parliament in its Resolution emphasised the need of an EU entity "tasked with ensuring compliance by content hosting platforms with the provisions of the regulation, in particular by monitoring compliance with the standards laid down for content management on the basis of transparency reports and monitoring algorithms employed by content hosting platforms for the purpose of content management".[374] Given the financial concerns in establishing an entirely new body,[375] an assessment had to be made on appointing an existing or new European Agency or body.[376] Finally, the DSA decided to implement an arrangement similar to that governing the privacy domain with national Data Protection Authorities (DPAs) in charge of applying the General Data Protection Regulation and a body made up of representatives of the national authorities, such as the Article 29 Working Party, and now the European Data Protection Board.[377] According to the DSA, Member States should designate one or more authorities competent for the enforcement of the Regulation, one of which should serve as Digital Service Coordinator (DSC) in the Member States.[378] The DSCs shall have broad powers spanning from ordering the cessation of infringements, imposing remedies to bring infringements to an end, to imposing fines, periodic penalty payments, and adopting interim measures to avoid serious harm.[379] The DSCs should make up an "European Board for Digital Services", and independent body tasked with advising the DSCs and the Commission on the application of the DSA and the supervision of VLOPs and VLOSEs.[380]

However, one pressing concern is the burgeoning number of regulatory bodies overseeing different aspects of digital governance. For instance, DPAs oversee the GDPR, DSCs are proposed for the DSA, and separate National Supervisory Authorities could be instituted for the EU AI Act. This multiplicity of bodies could lead to operational

[370]Ibid., Article 37.

[371]Ibid., Recital 91. See also EP Resolution on the DSA and commercial and civil law rules, see n. 95, point 12; EP Resolution on the DSA and the Single Market, see n. 94, point 41 and Annex to the Resolution, 28.

[372]Ibid., Annex to the Resolution, 29.

[373]See AI Act Proposal, see n. 30.

[374]EP Resolution on the DSA and commercial and civil law rules, see n. 95, point 8.

[375]It could be imagined that content hosting platforms which enjoy significant market power participate in the financing of independent dispute settlement bodies by making contribution to a fund created at the EU level. See EP Resolution on the DSA and commercial and civil law rules, see n. 95, Annex to the Resolution, pp. 19, 25–26.

[376]EP Resolution on the DSA and commercial and civil rules, see n. 95, point 8.

[377]See G. Sartor and A. Loreggia, *The impact of algorithms for online content filtering or moderation: Upload filters* (European Parliament, September 2020), 64.

[378]See DSA, see n. 16, Article 49. For recommendations for building a strong Digital Services Coordinator, see, J. Jaursch, 'Platform oversight: Here is what a strong Digital Services Coordinator should look like' (*Verfassungsblog*, 31 October 2022) <https://verfassungsblog.de/dsa-dsc>.

[379]Ibid., art 51.

[380]Ibid., arts 61–62. On the role of the Commission, see C. Krönke, 'Die Europäische Kommission als Aufsichtsbehörde für digitale Dienste', (2023) 24(2) *EuR* 136; more specifically, on the role of the Commission from a fundamental rights and democratic values perspective, see I. Buri, 'A Regulator Caught Between Conflicting Policy Objectives: Reflections on the European Commission's Role as DSA Enforcer' (*Verfassungsblog*, 31 October 2022) <https://verfassungsblog.de/dsa-conflicts-commission>.

silos and inefficiencies. It's worth considering whether these entities should be organised as units of a single body, similar for example to France's CNIL, which oversees both GDPR and AI regulations. Such an integrated approach would ensure *inter alia* that fundamental rights are consistently applied across different legislative frameworks.

In this regard, the establishment of a centralised, "independent EU oversight structure" with power to adopt decisions directly against DSPs, rather than national DSCs coupled with an EU advisory board, could be more effective in promoting regulatory harmonisation as well as the proper enforcement of the DSA.[381] Under the DSA scheme, national DSCs, or even possibly multiple national authorities, of the Member State of establishment of the DSP will be finally competent for receiving a complaint and issuing a decision, which might lead to forum shopping and political biases. This seems even more problematic given that recipients of the service can lodge a complaint against DSPs with the DSC of the Member State where they are established, while the complaint is later transmitted to the DSC of the Member State of establishment of the DSP. On top of the unnecessary complexity of this mechanism, different national DSCs might operate according to different policy approaches, resulting in a sub-optimal choice for addressing complaints from service recipients residing or established in different Member States.

Also, the DSA seems to construe this entity closer to an antitrust authority that oversees compliance of DSPs with DSA's obligations, rather than serving as guarantor of fundamental rights. Instead, for this purpose, this entity could work closely with the European Union Agency for Fundamental Rights.[382] As advocated previously in the field of copyright, a EU Council or a EU regulation authority should also ensure that ADR resolution mechanisms are available, in particular to secure fundamental rights of users.[383] Some quasi-judicial functions could also be assigned to this entity, for example acting as a dispute resolution body of last resort in the moderation cycle that will pick up borderline cases, whose adjudication might also serve as a precedent for DSPs moderation practices.[384] Such an EU entity might also help further qualifying what content is 'manifestly illegal', thus potentially subject to *ex ante* filtering. This would contribute to legal certainty as far as DSPs obligations might be concerned, thus strengthening protection of DSPs' freedom to conduct business within the DSA framework. In sum, the EU entity should be tasked with monitoring DSPs' compliance with the DSA, while at the same time identifying difficulties in implementation and issuing policy guidelines on how to remedy them, taking duly into account the fundamental rights impacted.[385]

In addition, an Ombudsperson might be entrusted with fundamental rights protection in dispute settlement proceedings reviewing content moderation. Such new functions could be conferred to the existing European Ombudsman,[386] an existing body, or a new institution. Either way, the Ombudsperson could act when a content hosting platform has decided to remove, take down or disable access to content, or otherwise to act in a manner that is contrary to the interest of the uploader or infringes fundamental rights'.[387] The Parliamentary Assembly of Council

[381]See EP Resolution on the DSA and commercial and civil rules, see n. 95, point 40. See also Nordemann and others, see n. 286, 303–307 (highlighting positive and negative impacts of a new regulatory agency); J.-P. Schneider et al., see n. 329, 43–55.

[382]An independent centre of reference for promoting and protecting human rights in the EU, to develop guidelines for a fundamental rights-compliant environment for platform liability, as established by the Council Regulation (EC) No 168/2007 of 15 February 2007.

[383]See in this sense, in particular in order to secure freedom of expression in the context of disputes around creative re-uses, C. Geiger, 'Freedom of Artistic Creativity and Copyright Law: A Compatible Combination?' (2018) 8(3) *UC Irvine Law Review* 413, 457. More generally, the idea of Copyright Council in the EU has been developed by Franciska Schönherr in her Ph.D. thesis under the direction of Christophe Geiger defended at the University of Strasbourg on 3 October 2017. See F. Schönherr, 'The Construction of an EU Copyright Law, Towards a Balanced Institutional and Legal Framework' (PhD thesis, University of Strasbourg 2017) and by N. Mangal, 'EU Copyright Reform: An Institutional Approach' (PhD thesis, University of Strasbourg, under the supervision of Christophe Geiger, defended 20 June 2022) (exploring the design of a new EU copyright institution, among other potential policy options). A EU independent authority has also recently been proposed in order to monitor platform liability in the context of the CDSM directive and to secure a fundamental rights-compliant implementation of art. 17 CDSM, see Geiger and Jütte, see n. 89; Geiger and Mangal, see n. 305.

[384]In any case, the concrete design, the exact scope of action and the merits of such an EU entity (which could tentatively be called "Digital Single Market and Ethics EU Observatory") would need further investigations. For an attempt to design the scope and function of such an institution in the field of copyright content moderation, see Geiger and Mangal, see n. 305.

[385]See EP Resolution on the DSA and commercial and civil rules, see n. 95, Annex to the Resolution, 13–14; Committee on Civil Liberties, Justice and Home Affairs, 'Draft Report on the Digital Services Act and fundamental rights issues posed' [2020/2022(INI)] 27 April 2020, PE650.509v01–00 <https://www.europarl.europa.eu/doceo/document/LIBE-PR-650509_EN.pdf>, point 21.

[386]The European Ombudsman was established by the Maastricht Treaty (1992). The role and powers of the European Ombudsman are currently regulated by Article 228 of the Treaty on the Functioning of the EU.

[387]See EP Resolution on the DSA and commercial and civil rules, see n. 95, point 11 and Annex to the Resolution, 26.

of Europe called on the European Union to consider whether to set up an Internet Ombudsman to foster harmonisation of legislation on internet content, while facilitating swift deletion of manifestly illegal content.[388]

However, independent oversight structures, Ombudspersons, possibly coupled with counter-notice procedures and out-of-court dispute settlements, should only complement, but never replace, proceedings before national courts.[389] The out-of-court dispute settlement mechanisms should in no way affect the rights of the parties to initiate legal proceedings and "effective judicial redress should remain available to satisfy the right to effective remedy".[390] In addition, decisions made by DSPs as to legality of the uploaded content should be provisional, and, as the EP recommended, "online intermediaries should not be held liable for it, as only courts of law should decide in the final instance what is illegal content".[391] The final decision on the legality of content must come from an independent judiciary, rather than private parties.[392] In sum, the use of digital services in the EU should be fully governed by EU law under the jurisdiction of Union courts.[393]

4.5 | Proportionality based on operational costs and dimensions

To foster market entry and growth for Small and Medium-sized Enterprises (SMEs),[394] any new obligations imposed on DSPs should be carefully calibrated to align with their scale, reach, and technical and operational capabilities.[395] This ensures that regulatory requirements are proportionate and do not inadvertently serve as barriers to SME participation in the market. In addition, proportionality should also look at potential harm that could stem from the activity of a DSP. In order to ensure proportionality, a balanced intermediary liability regime should subject only platforms with significant market power to the most pressing obligations, while other platforms should be exempted.[396]

The DSA endorses this graduate obligation approach by distinguishing between (i) providers of intermediary services, (ii) micro or small enterprises,[397] (iii) providers of hosting services, (iv) providers of online platforms, and (v) VLOPs and VLOSEs. Intermediary services are the broader category including access, caching, and hosting providers,[398] while 'online platforms' are hosting providers 'which, at the request of a recipient of the service, [store] and [disseminate] to the public information'.[399] Among online platforms, the DSA distinguishes between online platforms proper and online search engines, micro or small enterprises, which are excluded from additional obligations applicable to online platforms,[400] and VLOPs and VLOSEs, which are subject to stricter obligations than mere online platforms and search engines.[401] In particular, VLOPs and VLOSEs, as mentioned already, must assess risks in connection to (i) dissemination of illegal content though their services, (ii) negative effects on fundamental rights, and (iii) intentional manipulation of their services affecting public health, minors, civic discourse, elections, and public

[388]See Standing Committee of the Parliamentary Assembly of the Council of Europe, Resolution 2334 (2020), Provisional version, 'Towards an Internet Ombudsman institution', 15 September 2020, point 6, <https://pace.coe.int/en/files/28728/html>.
[389]See EP Resolution on the DSA and FRs, see n. 93, point 11 (noting that '[t]he ultimate responsibility for enforcing the law, deciding on the legality of online activities and ordering hosting service providers to remove or disable access to illegal content rests with independent competent authorities').
[390]EP Resolution on the DSA and FRs, see n. 93, point 29.
[391]EP Resolution on the DSA and the Single Market, see n. 94, Annex to the Resolution, 29.
[392]See EP Resolution on the DSA and commercial and civil law rules, see n. 95, point 5.
[393]ibid, point 39.
[394]See DSA, see n. 16, Recital 39, 'to avoid disproportionate burdens, those transparency reporting obligations should not apply to providers that are micro- or small enterprises as defined in Commission Recommendation 2003/361/EC'.
[395]See EP Resolution on the DSA and FRs, see n. 93, point 27. See also Article 19's Recommendations (n 288), Recommendations 7.
[396]See EP Resolution on the DSA and commercial and civil rules, see n. 95, point 3;EP Resolution on the DSA and the Single Market, see n. 94, Annex to the Resolution: Recommendations as to the Content of the Proposal Requested, 32–33.
[397]Within the meaning of the Annex to Recommendation 2003/361/EC.
[398]Ibid., Article 3(f).
[399]Ibid., Article 3(i) ("unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons, cannot be used without that other service").
[400]See DSA, see n. 16, Article 19.
[401]Ibid., Article 33.

security.[402] Afterwards, if it is the case, VLOPs and VLOSEs must put in place mitigation measures as a result of their risk assessment,[403] and independent audit.[404]

By 17 February 2023, platforms were required to disclose their user base in Europe. Those boasting more than 45 million users—equating to 10% of the European populace—are designated as VLOPs or VLOSEs.[405] These digital behemoths are, by virtue of their reach, subject to intense scrutiny by European regulators, and had to adhere to DSA obligations within four months of their designation, which occurred on 24 April 2023. Meanwhile, all other platforms have until February 17, 2024, to fully align with the DSA's guidelines. Nineteen key online platforms and search engines—ranging from social media giants like Facebook and Twitter to e-commerce sites like Amazon and Alibaba—have been mandated to submit their initial online risk assessments. Failure to adhere to the DSA's stipulations within the designated timeline could result in penalties amounting to as much as 6% of the company's annual revenue. While the list of VLOPs designated by the Commission includes eight social networks (Facebook, TikTok, Twitter, YouTube, Instagram, LinkedIn, Pinterest, and Snapchat), five e-commerce platforms (Amazon, Booking, Alibaba AliExpress, Google Shopping, and Zalando), Apple and Google app stores, Google Maps, and Wikipedia, notable absentees like eBay, Airbnb, Netflix, and PornHub could find themselves included in future iterations of the DSA's regulatory framework. The Commission designated also two VLOSEs, Bing and Google Search.

To strike a balanced compromise among multiple stakeholders, the DSA wisely adopts a proportional approach to the obligations imposed on DSPs. This approach aims to delicately balance the fundamental rights of various parties involved: users' freedom of expression, online businesses' freedom to conduct a business, and the intellectual property rights of content creators and owners. Particularly in the context of VLOPs, where infringement on a massive scale poses significant threats to rights holders, a proportionate regulatory framework helps to uphold these fundamental rights while also acknowledging the complexities of the digital landscape.[406]

5 | CONCLUSIONS: RECOMMENDATIONS FOR A FUNDAMENTAL RIGHTS-CENTRED PLATFORM LIABILITY REGIME

1. The regulation of DSPs in contemporary information societies raises a number of ethical and social challenges. Certain DSPs play a crucial role in facilitating public access to information and shaping interaction around it, thus serving a key democratic function. They act as conduits for user speech, creativity, and the exchange of ideas. Fundamental Rights should be central to any discourse on DSP regulation, as they provide essential protections for democracy and the rule of law. These rights also hold a high standing in the European Union's normative hierarchy, shaping all secondary legislation. Historically, regulation concerning intermediary and platform liability have grappled with striking the right balance between the conflicting rights affected by DSPs' activities and obligations.
2. The DSA represents a concerted effort to balance a myriad of conflicting interests while upholding fundamental rights. Although it introduces innovative regulatory mechanisms for platform governance, it is an exceptionally intricate and lengthy legislative document, where preference for national oversight strategies over unified European approaches risks further complicating its harmonised implementation. Given these complexities,

[402]Ibid., Art 24.
[403]Ibid., Art 35.
[404]Ibid., Art 37.
[405]European Commission, Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines, Press Release, 25 April 2023.
[406]Article 17 of the C-DSM Directive could have taken a cue from the DSA by focusing its licensing and content removal obligations solely on very large online platforms (VLOPs). Instead, Article 17(6) exempts only a narrow group of emerging platforms in the initial stages of market growth from its most stringent requirements. This approach leaves the majority of startups, which might not yet have the resources to comply, burdened with content-filtering obligations. This raises questions about proportionality and the potential stifling of innovation within the digital ecosystem. See Directive 2019/790/EU, see n. 11, Article 17. See also Frosio, 'Reforming the C-DSM Reform'see n. 196, 721, 727–728 (examining the adverse impact of the new obligations in the C-DSM Directive on start-ups and smaller platforms).

subsequent revisions and fine-tuning will inevitably be required to best protect fundamental rights in our rapidly evolving digital landscape. In this respect, the theoretical framework of "digital constitutionalism" may offer valuable insights and guidance.

3. Past frameworks, such as the ECD, have established limited liability regimes that included exemptions for DSPs, offering robust safeguards for users' fundamental rights. Recent modifications to this paradigm have been introduced through the C-DSM Directive. In this evolving landscape, the DSA deserves praises for its careful effort to preserve the ECD long-standing balance of fundamental rights. Rather than disrupting this equilibrium, the DSA accentuates the importance of fundamental rights online, taking very seriously the task of safeguarding the fundamental rights of users, platforms, and other affected parties.
4. As advanced in this article, a proportional balancing of fundamental rights within the DSA reform should primarily draw upon the legal foundations established by the ECHR and the EU Charter. These foundational texts should be interpreted in light of the case law from the ECtHR and the CJEU. Incidentally, the international human rights framework could serve as an additional reference, as courts often draw inspiration from these treaties when defining the European standards for the protection of fundamental rights. Against this backdrop, several key challenges come into focus:

- First, it is essential to avoid imposing additional limitations on freedom of expression, which encompasses freedom to receive information and internet access, freedom to impart information, and freedom of the arts. Any restrictions that significantly curtail online access to information would inadequately safeguard user rights. These rights are deeply rooted in fundamental rights, as evidenced by cases involving wholesale website blocking, excessive removal of legal content, or the disproportionate use of algorithmic filtering tools. Meanwhile, it is important to note that the extent of permissible limitations on freedom of expression can vary based on the nature of the content, Certain types of content, such as hate speech and speech inciting violence, may be entirely excluded from protection.
- Secondly, mandating filtering and monitoring obligations for DSPs runs afoul of the right to privacy and data protection. These rights serve as a counterbalance to the interests of both DSPs and rightholders in processing data for monitoring, filtering, and other purposes. CJEU decisions, such as *Netlog*, *Scarlet* or *Google Spain*, inhibit the wholesale. processing of user data that might occur in general monitoring and filtering, or other processes; nonetheless public interest information must always remain accessible. In such instances, the right to freedom of expression and the freedom to access information take precedence.
- Thirdly, private entities should not be permitted to encroach upon due process standards in their decision-making and enforcement actions. To safeguard fundamental rights during dispute resolution between users and platforms, there must be full transparency and explicitly defined procedural rights. The push for the broad use of algorithmic enforcement tools exacerbates the inherent tension between private ordering and traditional due process norms.
- Fourthly, obligations that are disproportionate, like the mandate for filtering mechanisms, incur substantial financial and human resource costs. This can potentially undermine DSPs' freedom to conduct business and create barriers to market entry for SMEs and start-ups. Therefore, it is crucial that independent public bodies play an active role in determining and implementing content removal criteria, rather than relegating this responsibility and burden solely to private entities.
- Finally, while the intellectual property rights of rightsholders must always be taken into account in any balancing exercise—as is the case with any property right—these rights are not absolute and must be tempered by public interest limitations. The EU legislator possesses considerable latitude in shaping the scope of IP enforcement tools, especially when significant competing fundamental rights are involved.

5. The DSA aptly underscores that, while aspects of the legal framework established by the ECD may benefit from modernisation, several of its existing provisions continue to serve as vital safeguards for fundamental rights.

Specifically, the ECD's *ex post* "knowledge-and-take-down" mechanism should generally be favoured over proactive, *ex ante* content moderation due to its stronger protection for users' rights. it is thus crucial for the DSA to maintain the prohibition against general monitoring obligations, consistent with its legislative predecessors, specifically Article 15 of the ECD and Article 17(8) of the C-DSM Directive. Such obligations could overly constrain users' freedom of expression and access to information, while placing undue burdens on service providers. In the context of a proportionality assessment, exceptions to this principle should be rare and limited to specific scenarios, such as the removal of manifestly illegal content that doesn't require independent assessment.[407] Especially in the context of intellectual property enforcement, automated filters should not be solely relied upon to fulfil the content moderation responsibilities of DSPs. Given the current technological limitations, such tools are ill-equipped to discern between legitimate and illegitimate usage effectively.[408] Consequently, adherence to the "human-in-command" principle is imperative to ensure nuanced and accurate content moderation.

6. The DSA choses the right policy approach by not regulating harmful content, but rather harmonising rules for tackling illegal content. From a freedom of expression perspective, controversial content cannot be censored just because it makes the audience uncomfortable. However, differing regulatory approaches should be applied to illegal and manifestly illegal content. **(i)** In addition to content that promotes offences against human dignity, war crimes, crimes against humanity, human trafficking, incitement to or apology of violence, acts of terrorism, and child abuse, the category of "manifestly illegal content" could also include content that blatantly infringes on intellectual property rights, where no equity-based assessment is needed. In this particular context, any content that could potentially be considered as a privileged use, or whose legality might be open to interpretation, should never be classified as "manifestly illegal". Manifestly illegal content merits fewer protections and can be expediently removed through streamlined procedures and, where appropriate, automated tools The DSA, or an independent regulatory body, should clearly delineate what qualifies as "manifestly illegal" to avoid ambiguities. **(ii)** Instead, for content that is illegal but not manifestly so, and therefore whose illegality must be assessed, human review to assess its legality should be mandatory. Further independent scrutiny should also be available upon request. Consistent standards, including expeditious removal within a reasonable timeframe, must be adhered to in all circumstances. **(iii)** As for content that is harmful but not illegal, outright removal is not the most prudent course of action from a freedom of expression standpoint. Alternative strategies like content flagging by DSPs and users, or other counter-speech mechanisms, such as "like" or "dislike" buttons, should be explored. Furthermore, users should have more agency in customising what type of content they wish to engage with.
7. Enhanced procedural guarantees for content moderation better safeguard fundamental rights. In this context, **(i)** users should have increased access to information about content curation and moderation practices, including the ability to opt-out of unwanted content curation. **(ii)** Consistent with the DSA's approach, establishing an efficient, and long awaited, notice-and-action mechanism is crucial for the safeguard of fundamental rights online. This mechanism must feature procedural safeguards for those flagging potentially illegal content (notice providers), those whose content is flagged (content providers), and other interested parties. It should also facilitate the swift reinstatement of unjustly removed content. **(iii)** Except for instances involving manifestly illegal content, content that has received a notice should remain accessible while its legality is under review, unless a judicial or administrative order mandates its removal; meanwhile, during this assessment period, DSPs should be exempt from liability for opting not to remove the content. **(iv)** Lastly, transparency and human oversight must be integral to the decision-making process, ensuring that all parties have access to independent dispute resolution mechanisms and judicial remedies.

[407] As the European Copyright Society has underlined, 'Recital 28 DSA confirms that obligations imposed on providers to monitor in specific cases are not against the ban of Art. 7 DSA. The DSA does not specify the line between general and specific monitoring, leaving this task largely to the CJEU, as was the case up until now'. A. Peukert and others, 'European Copyright Society: Comment on Copyright and the Digital Services Act Proposal', 367.

[408] See in this sense also C. Geiger and B. J. Jütte, 'Towards a Virtuous Legal Framework for Content Moderation by Digital Platforms in the EU? The Commission's Guidance on Article 17 CDSM Directive in the light of the YouTube/Cyando judgement and the AG's Opinion in C-401/19', (2021) 43(10) *European Intellectual Property Review*, 615 ff.

8. Under the DSA, the EU has taken pioneering steps to introduce specific regulations surrounding the use of algorithmic tools in content moderation, with an emphasis on safeguarding fundamental rights. Importantly, the DSA does not mandate DSPs to employ algorithmic tools; however, if DSPs choose to use such tools, they must adhere to stringent guidelines. These guidelines include: **(i)** transparency and non-discrimination in algorithmic processes; **(ii)** mandatory human review for algorithmic decisions, **(iii)** periodic audits and external oversight to ensure compliance with DSA's standards; (iv) risk assessment and mitigation protocols, particularly concerning threats to fundamental rights due to the design of algorithms, for VLOPs and VLOSEs, and **(v)** yearly transparency reports detailing algorithmic content moderation and enforcement activities. However, the DSA's approach to algorithmic transparency and accountability could be refined further. To counter the challenges of algorithmic opacity and the so-called "black box society", more specific obligations could be introduced. These could address issues such as algorithmic bias, which may result in 'echo chambers' where users are exposed only to reinforcing content. Other enhancements could involve providing clearer explanations for automated decision-making logic, transparency around data sets used for algorithmic training, and robust redress mechanisms to handle the potential harm arising from algorithmic decisions. Overall, these additional measures would contribute to greater algorithmic accountability.
9. To effectively navigate the intricate legal challenges in an ever-changing technological environment, the DSA proposes specialised institutional oversight bodies responsible for monitoring DSPs' compliance. However, these entities should also champion the safeguarding of fundamental rights within the digital services ecosystem. **(i)** Specifically, a separate, centralised, independent EU entity should oversee the DSA's implementation, rather than leaving it to national bodies like the Digital Services Coordinators. The reason is twofold: first, to ensure a harmonised approach across Member States; and second, to efficiently manage the complex regulatory landscape of content moderation in the digital era. Operating in close partnership with the European Union Agency for Fundamental Rights, this proposed EU body—tentatively named the "Digital Single Market and Ethics EU Observatory"—should identify implementation challenges and offer policy guidelines to address them, always with due regard to the impact of fundamental rights impacted. **(ii)** Beyond its monitoring functions, this centralised EU entity could also serve quasi-judicial functions in online content moderation. For example, it could act as a final dispute resolution authority after the exhaustion of out-of-court dispute settlement mechanisms stipulated in the DSA. This entity could take up borderline cases whose resolutions might set precedents for future moderation practice by DSPs. However, the availability of such dispute resolution should not preclude users from instituting proceedings before an independent judiciary. **(iii)** Finally, an Ombudsperson could be vested with the authority to represent users in these proceedings, ensuring their rights are sufficiently protected.
10. Finally, DSPs' obligations should adhere to the principle of proportionality and legal certainty, Additionally, these obligations and should not inhibit the freedom to conduct business by introducing impractical or ambiguous requirements. Importantly, care must be taken to avoid creating entry barriers for SMEs. Any obligations should be tailored to DSPs' technical and operational capacities. In this regard, the DSA offers a nuanced approach to assigning obligations, liability and responsibility to DSPs based on factors such as their size and market share. This represents a significant stride forward in internet and intermediary liability regulation. As we look toward the future, this nuanced allocation should serve as a benchmark for any regulatory framework concerning content moderation online.

How to cite this article: Frosio G, Geiger C. Taking fundamental rights seriously in the Digital Services Act's platform liability regime. *Eur Law J*. 2023;29(1-2):31-77. doi:10.1111/eulj.12475