Review of European and Comparative Law | 2024
Vol. 59, No. 4, 149–175
https://doi.org/10.31743/recl.17528
Received: 4 June 2024 | Accepted: 4 September 2024 | Published: 20 December 2024

A New Legal Framework for Online Platforms in the European Union (and Beyond)

Julián López Richart
PhD, Associate Professor, Faculty of Law, University of Alicante (Spain); correspondence address: Faculty of Law, University of Alicante, Campus de San Vicente s/n, Ap. 99, 03080 – San Vicente (Alicante); e-mail: julian@ua.es
https://orcid.org/0000-0003-3998-5858

Keywords:
Internet regulation, intermediary service providers, online platforms, liability

Abstract: In the early 2000s, the EU adopted the Electronic Commerce Directive to regulate information society service providers. An important part of this piece of legislation was the safe harbor provisions, which exempted intermediary service providers from liability for illegal content transmitted or hosted by their users, provided that they complied with specific conditions. After more than twenty years, the emergence of significant online platforms and the increased use of those services has resulted in new risks and challenges for individuals, companies, and society as a whole, which led the European Union to adopt a new regulatory framework for intermediary services. The Digital Services Act retains the liability exemption regime of the Electronic Commerce Directive but introduces new transparency and due diligence obligations for intermediary services, especially for online platforms. The new regulatory framework is expected to substantially impact globally, as it applies to all intermediary service providers offering services within the EU, regardless of their location. This study explores the main features of the DSA and their potential effects on the future development of the Internet.

ISSN 2545-384X (Online)

1. Introduction

More than 20 years have passed since the Electronic Commerce Directive (hereinafter ECD)[1] adopted a legal framework to regulate the activity of information society service providers. Among many issues, in order to encourage innovation and the development of the Internet, the ECD established a regime of exemption from liability for intermediary service providers (ISPs), including hosting service providers. The latter would be exempted from liability for illegal content hosted by service recipients provided that they had no actual knowledge of the illegality or, if they had such knowledge, that they acted promptly to remove or disable access to it. The regulation left many questions open, which case law tried to resolve while adapting a regulation meant for a very different economic and technological environment. The prominence acquired by online platforms in recent years and the risks they entail for Internet users and society as a whole have led the European Union legislator to intervene, adopting a new regulatory framework for Internet service providers in the Regulation (EU) 2022/2065 on a Single Market for Digital Services,[2] known as the Digital Services Act (DSA).

The DSA essentially maintains the liability exemption regime existing in the ECD but introduces significant new features in terms of transparency and duties of diligence for online platforms, in particular, for the very large ones. This new legal framework is expected to have a significant impact not only within the European Union but also globally since the new rules apply to intermediary service providers, regardless of their place of establishment or location, to the extent that they offer services in the Union.

---

1 Directive (EU) No. 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (O.J.E.C. L178, 17 July 2000), 1–16, accessed June 4, 2024, https://eur-lex.europa.eu/eli/dir/2000/31/oj.

2 Regulation (EU) No. 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (O.J.E.C. L277, 27 October 2022), Document L: 2022:277:TOC, accessed June 6, 2024, https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

2. The Shortcomings of the Electronic Commerce Directive Twenty Years Later

2.1. The Origin of the Safe Harbor Provisions and Their Impact on the Development of the Platform Economy

The origin of the exemption from liability of ISPs dates back to the late 1990s when the United States Congress passed the Communications Decency Act (CDA) of 1996 to resolve inconsistencies in previous judicial decisions and prevent intermediaries who take measures to prevent the commission of unlawful conduct through their services from being subject to a stricter liability regime than those who do not. In this regard, section 230 CDA laid down that the provider of an interactive computer service shall not be regarded as the publisher or originator of the information supplied by the provider of such content, nor could it be held liable for any action taken in good faith to restrict the availability of illegal content. This provision, coupled with the courts' broad interpretation, has effectively granted ISPs virtually absolute immunity.[3] However, certain matters are expressly excluded from the scope of application of the provision, such as federal crimes and trademark or copyright infringements.

Two years later, the Digital Millennium Copyright Act (DMCA) established a specific immunity regime for ISPs concerning copyright infringements. This regime is more nuanced than that of the CDA, which may be explained by the fact that, on this occasion, the telecommunications sector clashed with an equally powerful lobby, namely the content industries. The DMCA thus enshrined a compromise, which resulted in the establishment of a series of conditions under which ISPs were exempt from liability for copyright infringements committed by their users. These conditions, known as "safe harbors," depend on the type of service these intermediaries may perform (transmission of data, caching, storage and linking). Nevertheless, the liability exemption of ISPs under both the DMCA and the CDA responded to the same legislative policy decision: preventing the risk of

[3] On this question, for the criticism of the scope that the case law has given to section 230 CDA, see: Neville L. Johnson et al., "Defamation and Invasion of Privacy in the Internet Age," *Southwestern Journal of International Law* 25, no. 1 (2019): 12 ff.

liability became a disincentive to those who should be driving the emerging development of the Internet.[4]

The same concern that led the US legislator to protect ISPs is behind the creation of the ECD, which was adopted to promote the development of information society services.[5] In Europe, there was another equally important policy reason for regulating the liability of ISPs, though. The European legislator was concerned about the emerging disparity in the criteria applied in national jurisdictions regarding the liability of intermediary service providers, which was perceived as a potential obstacle to the proper functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition.[6] To overcome this regulatory disparity, the ECD followed the approach adopted two years earlier by the DMCA by merely providing liability exemption rules instead of attempting to harmonize the liability regime applicable to intermediary providers for the content transmitted or stored by their users, a task that would probably have been impossible to achieve, given the different legal traditions and doctrines applicable at a national level. The attribution of liability of intermediary service providers would, therefore, continue to depend on the substantive rules applicable in the different national systems,[7] where there might be (and indeed are) significant divergences.[8] The ECD only imposed on Member States the obligation to ensure that, in any case, and whatever the applicable national regime, intermediary service providers would be exempted from liability provided

4 It has been argued that section 230 CDA was key for the development of the Internet as we know it, see: Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Ithaca, London: Cornell University Press, 2019).

5 Recital 5 ECD.

6 Recital 40 ECD. On the existing state of affairs in the Member States prior to the adoption of the Directive, see: Rosa Julià Barceló, "Liability for On-line Intermediaries. A European Perspective," *E.I.P.R.*, no. 12 (1998): 456 ff.

7 See: CJEU Judgment of 11 September 2014, Sotiris Papasavvas v. O Fileleftheros Dimosia Etaireia Ltd and Others, Case C-291/13, ECLI:EU:C:2014:2209, 53.

8 As an authorized spokesperson of the European Commission said at the time of the adoption of the ECD, "[the Directive] determines only those cases in which a provider may benefit from an exemption or limitation of liability. This does not mean that the provider will necessarily incur liability if it does not comply with these conditions. In this case, the national liability regime will apply to determine the provider's liability," see: Emmanuel Crabit, "La directive sur le commerce éléctronique," *Revue du Droit de l'Union Européenne*, no. 4 (2000): 812.

that they comply with certain specific conditions, which vary depending on the type of service.

In this respect, the ECD distinguished three types of services: mere transmission (Article 12), caching (Article 13), and hosting (Article 14), defining for each the conditions under which those who transmitted, cached, or hosted content provided by the recipients of their services were exempted from liability. Undoubtedly, the most problematic in practice was the latter, partly because of the relevance that content hosting services gained with the emergence of Web 2.0, but mainly because the contours of their liability exemption were rather vague. Under Article 14 ECD, hosting providers were exempt from liability if they had no actual knowledge or awareness of the facts and circumstances from which the illegal activity or information was apparent. Hosting providers were also exempted from liability if they acted expeditiously to remove or disable access to the information upon obtaining such knowledge or awareness.

Furthermore, Article 15 ECD provided that Member States may under no circumstances impose on intermediary service providers a general obligation to monitor the information they transmit or store, nor a responsibility to actively seek facts or circumstances indicating illegal activity. This prohibition of imposing a general monitoring obligation does not affect the possibility of Member States requiring ISPs to apply the duty of care that can reasonably be expected from them and specified by national law to detect and prevent certain types of illegal activities.[9]

Even though the ECD was inspired by the US DMCA, there were significant differences.[10] First of all, the ECD adopted a horizontal approach to the extent that the safe harbor provisions apply to all types of unlawful activities (not only to civil copyright infringements), irrespective of the precise subject matter and the type of liability deriving from it.[11] Secondly,

[9] Recital 48 ECD. For the distinction between general and specific monitoring obligations, see: CJEU Judgment of 3 October 2019, Eva Glawischnig-Piesczek v. Facebook Ireland Limited, Case C-18/18, ECLI:EU:C:2019:821.

[10] For a detailed analysis of the differences between the two norms, see: Miquel Peguera Poch, "The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems," *Colum. J. L. & Arts* 32, (2009): 481 ff.

[11] It should be noted that the horizontal nature of the rules of exemption from liability of the ECD has recently been broken with the approval of Directive (EU) No. 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital

the Directive did not include a liability exemption for providers of linking services and search engines. Whereas the DMCA articulates a mechanism (subpoena) whereby rightsholders can require the ISPs to identify the provider of the allegedly infringing content,[12] the Directive did not require service providers to disclose the identity of their users.[13] Finally, although the European Directive did not establish when or how the service provider could become aware of the infringing content. In comparison, the DMCA lays down a "notice and takedown" procedure so that any interested person can bring it to the attention of the hosting service provider. Only if this notice procedure is followed and the service provider does not remove the content can the latter be held liable.

Nonetheless, many of the arguments that initially justified the exemption of liability for ISPs – especially for hosting providers – have been fading away due to the evolution of the Internet over the past 20 years.[14]

Firstly, safe harbor provisions were based on the assumption that it would be materially impossible for ISPs to check the legality of all the information they transmit or host since they handle millions of users. The information that passes through their system is just a sequence of bits, that is, a succession of 0's and 1's, which, without further processing, obscures the real meaning of the information itself. Besides, even if they could, it would possibly be illegal for them to assess the legality of this information

Single Market and amending Directives 96/9/EC and 2001/29/EC (O.J.E.C. L130, 17 May 2019, accessed June 6, 2024, https://eur-lex.europa.eu/eli/dir/2019/790/oj), which excludes the application of Article 14 ECD with respect to a very specific category of hosting service providers. i.e. online content-sharing platforms, with regard to infringements of copyright or related rights deriving from the content uploaded by their users.

12 Outside the scope of application of the Copyright Act, when the aim is to identify the author of allegedly defamatory comments, US courts are reluctant to consider requests addressed to ISPs to disclose the identity of their users, arguing that the court must weigh the arguments and evidence presented by the plaintiff against the constitutionally protected right of the alleged infringer to express himself anonymously. In that regard, see: *Dendrite Int'l, Inc. v. Doe No. 3*, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

13 Nevertheless, EU law does not preclude Member States from imposing upon service providers a duty to provide competent authorities information enabling the identification of the user behind illegal content, see: CJEU Judgment of 29 January 2008, Productores de Música de España (Promusicae) v. Telefónica de España SAU, Case C-275/06, ECLI:EU:C:2008:54, 54.

14 See: Lilian Edwards, "'With Great Power Comes Great Responsibility?': The Rise of Platform Liability," in *Law, Policy and the Internet*, ed. Lilian Edwards (Oxford: Hart, 2019), 257–61.

without invading the privacy and confidentiality of their subscribers. However, technical mechanisms are being developed to detect infringing and illegal material and prevent it from being transmitted or uploaded in the first place. Filtering technology is still far from perfect, but machine learning and artificial intelligence (AI) might help to make such systems much more accurate, even in areas like libel and hate speech, where semantic meaning has been so far dependent on human interpretation.[15]

Secondly, the idea that hosting service providers, like other ISPs, are totally unrelated to the content that their users store on their servers may hold true with regard to the service model they typically provided when the ECD was drafted, long before the emergence of social networks and the development of Web 2.0. However, the emergence of social networks and other user-generated content platforms has raised the question of whether they really deserve to be treated as simple carriers or distributors of information and not as publishers of content provided by third parties, since they have control over the dissemination of the information they store, and they use this power to promote their business. Indeed, their entire business model is based on monetizing user data and attention, and thus the amount of information hosted, its content, and how it is presented and ranked is no longer irrelevant for the service provider.

Finally, the initial approach to the liability of ISPs was based on the assumption that the promotion of e-commerce and the information society required the development of new and innovative services and the involvement of the emergent ISP industry in order to expand Internet infrastructure. Making this market more attractive and creating a safe environment for start-ups and innovators to grow a feeling of safety against liability claims were key. This narrative could be plausible in the mid- and late-1990s but not today, particularly concerning the big players from Silicon Valley and large companies that dominate global markets, such as Meta, Google, or Amazon.

[15] With regard to the possibility that an automated system would be able to properly apply the doctrine of fairness to copyright, see: Niva Elkin-Koren, "Fair Use by Design," *UCLA Law Review* 66, (2017): 1097–9.

2.2. The Role of the Court of Justice in Shaping the Liability Regime of Online Platforms

In response to the evolution of hosting service providers, the Court of Justice was asked on different occasions whether new services were eligible for the liability exemption under Article 14 ECD, which led to the delimitation of the concept of hosting service provider.

The question was first raised before the Court of Justice in the Google France case in which the CJEU was asked, among other things, whether the search engine could rely on the exemption from liability rule of Article 14 ECD if advertisers using Google's AdWords service were found to be infringing a trademark. In his opinion, Advocate General Poiares Maduro had considered that, unlike the natural results of Google searches, which are underpinned by automatic algorithms that apply objective criteria to generate websites that may be of interest to the user,[16] the AdWords service offered by the search engine is not a neutral vehicle of information since it takes place in an advertising context in which Google has a direct interest so that the exemption from liability for data hosting under Article 14 ECD should not be applied.[17] The Court of Justice of the European Union (CJEU) did not follow the Advocate General's reasoning. Despite embracing the requirement of neutrality as a determining factor, it did so with a different meaning. Based on recital 42 ECD,[18] the Court concluded that, for a hosting service provider to fall within the scope of Article 14 ECD, the provider must be an "intermediary" within the meaning intended by the legislator in the title of Section 4 of Chapter II of that Directive, which depends on whether the role played by that service provider is merely technical, or instead it plays an active role of such a kind as to give it knowledge of, or control over, the information provided by their users.[19] However,

16 Opinion of Advocate General Poiares Maduro, delivered on 22 September 2009, Joined Cases C-236/08, C-237/08 and C-238/08 (Google France), ECLI:EU:C:2009:569, 144.

17 Ibid., 145.

18 Recital 42 ECD provides that the exemptions from liability only apply to cases where 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."

19 CJEU Judgment of 23 March 2010, Google France SARL and Google Inc. v. Louis Vuitton Malletier SA, Google France SARL v. Viaticum SA and Luteciel SARL, and Google France

the mere fact that the referencing service is subject to payment, that Google sets the payment terms or that it allows for general information to its customers cannot have the effect of depriving Google of the exemptions from liability provided for in Article 14 ECD.[20]

The neutrality requirement has been the subject of much criticism. It has been said that it breaks the delicate balance established by the ECD,[21] which is not supported by the text of the Directive itself, and that could lead to divergent interpretations by national courts.[22] Some commentators have pointed out that the source of the confusion is the unfortunate wording of recital 42 ECD, which gives the impression that it refers to the three categories of intermediation service providers referred to in Section 4 of Chapter II ECD, when, in fact, it only refers to activities of mere conduit and proxy caching, which are purely technical, automatic, and passive.[23]

Advocate General Jääskinen was particularly critical of the neutrality requirement in his opinion on the L'Oréal case, which originated in an action brought by the well-known cosmetics brand against eBay after finding that counterfeit products were being marketed in the UK via eBay's website. L'Oréal claimed that eBay was liable for infringement of its trademarks, both by displaying those products for sale on its website and by the fact that eBay had placed advertisements through Google's AdWords service to promote some of them. The Advocate General considered that "'neutrality' does not appear to be quite the right test under the directive for this

SARL v. Centre national de recherche en relations humaines (CNRRH) SARL and Others, Joined Cases C-236/08 to C-238/08, ECLI:EU:C:2010:159, 114.

20 Ibid., 116.

21 Ian Walden, "Mine Host Is Searching for a 'Neutrality' Principle!," *Computer Law & Security Review* 26, no. 2 (2010): 208–9.

22 Stéphane Lemarchand and Marion Barbier, "Le fournisseur d'hébergement au sens de l'article 14 de la directive 2000/31 e la (nouvelle?) condition de neutralité," *Revue Lamy Droit de l'Immatériel*, no. 54 (2009): 54–6; Sophie Stalla-Bourdillon, "Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well," in *The Responsibilities of Online Service Providers*, eds. Mariarosaria Taddeo and Luciano Floridi (Cham: Springer, 2017), 280–1.

23 Patrick van Eecke, "Online Service Providers and Liability: A Plea for a Balanced Approach," *Common Market Law Review* 48, no. 5 (2011): 1482; the author is arguing that, unlike mere transmission or caching activities, which are passive, the activity of hosting service providers implies a certain degree of involvement with the conduct of their users, so it is incorrect to make its exemption from liability dependent on the requirement of neutrality.

question" and that "[he] would find it surreal that if eBay intervenes and guides the contents of listings in its system with various technical means, it would by that fact be deprived of the protection of Article 14 regarding the storage of information uploaded by the users."[24] In his view,

> provided that the listings are uploaded by the users without any prior inspection or control by the electronic marketplace operator involving interaction between natural persons representing the operator and the user, we are faced with the storage of information which is furnished by a recipient of the service.[25]

However, the Advocate General considered that the answer would be different if the same hosting provider carried out other activities which do not consist of data storage and are therefore not covered by Article 14. In this respect, after recalling that Articles 12, 13 and 14 ECD provide for exemptions from liability for certain types of activity and not for a certain type of service provider as such, he stated that "the hosting of the information provided by a customer may well benefit from an exemption if the conditions of Article 14 ECD are satisfied. Yet the hosting exception does not exempt eBay from any potential liability it may incur in its use of a paid internet referencing service."[26] In short, the Advocate General said that if it could be proved that eBay selected certain sale offers and used them to promote its website through Google's AdWords, it would have acted as a content provider and not as a mere intermediary.

Despite the criticisms, the Court of Justice confirmed the requirement of neutrality as a defining element of an intermediary. However, the conclusion it reached is not very different from that of the Advocate General. Indeed, after insisting that the provider of a hosting service is only covered by Article 14 ECD when it plays a neutral position with regard to the data provided by its customers, it points out that the mere fact of storing sale offers on its server, determining the conditions of its service, receiving remuneration in exchange for the service, or providing general information

---

24 Opinion of Advocate General Jääskinen delivered on 9 December 2010, Case C-324/09 (L'Oréal), ECLI:EU:C:2010:757, 146.

25 Ibid., 143.

26 Ibid., 151.

to its customers, are not criteria which, in themselves, allow the provider to be considered to have played an active role. On the contrary, if an operator provides assistance consisting of optimizing the presentation "of certain sales offers" or promoting "such offers," it is no longer possible to speak of purely technical and automatic processing of data provided by its customers, but an active role enabling it to acquire knowledge or control of the data relating to those offers.[27]

Therefore, in the light of the jurisprudence, the neutrality requirement does not mean that hosting providers should be completely passive towards the information hosted by their users, let alone that 2.0 hosting providers should, by definition, be excluded from the protection offered by Article 14 ECD. The constant references made by the Court of Justice to the specific infringing content and the connection of the neutrality requirement with knowledge and control over the content hosted by third parties seem to indicate that the Court of Justice is seeking to distinguish between intermediaries who maintain their independence from the infringing content and those who, on the contrary, take sides with such content to the point of being participants in the infringement, which is what makes them not deserving of protection.[28] With regard to providers of mere conduit and caching services, recital 44 ECD states that "a service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of 'mere conduit' or 'caching' and as a result cannot benefit from the liability exemptions established for these activities" and the same should apply to hosting providers.

The Court of Justice has recently clarified that the fact that the operator of an online content-sharing platform automatically indexes content

---

27 CJEU Judgment of 12 July 2011, L'Oréal SA and Others v. eBay International AG and Others, Case C-324/09, ECLI:EU:C:2011:474, 115–6.

28 See: van Eecke, "Online Service Providers," 1463; Tatiana-Eleni Synodinou, "Intermediaries' Liability for Online Copyright Infringement in the EU: Evolutions and Confusions," *Computer Law & Security Review* 31, (2015): 65; Giovanni Sartor, "Providers Liability: From the eCommerce Directive to the Future. In-Depth Analysis for the IMCO Committee," October 2017, 26, accessed June 4, 2024, https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf. These authors argue that the idea that only hosting service providers who take a passive role are shielded from liability should be abandoned, in particular if indexing content uploaded by users or providing search tools is to be considered as an active action.

uploaded to that platform, has a search function, or recommends videos based on users' profiles or preferences is not sufficient ground to conclude that it plays an active role and therefore loses the protection granted by Article 14 ECD to hosting providers.[29]

2.3. Online Harms as the Driving Force Behind the Regulation of Intermediaries

All in all, what actually led the European lawmakers to intervene was the realization that intermediaries, mostly online platforms and social networks, are not only a channel of expression and access to information that contribute to the democratization of public discourse but also carry serious risks for individuals and society as a whole. Beyond their obvious benefits, social media have been increasingly used over the last two decades to disseminate illegal and harmful content, spread misinformation, or influence electoral processes. There is extensive evidence that the architecture behind some online platforms is part of the problem. Moreover, despite the technology-neutral approach of the ECD, it became apparent that its provisions were no longer sufficient to address the challenges of modern digital reality. New rules were needed to keep up with the overwhelming evolution of digital technology and the transformation of business models.[30]

Initially, the European Commission focused on promoting self-regulation under Article 16 ECD. On September 28, 2017, the Commission adopted a Communication with guidance on the responsibilities of online service providers in respect of illegal content online.[31] In that Communication, the Commission explained that it would assess whether additional measures were needed, inter alia, by monitoring progress on the basis of

---

29 CJEU Judgment of 22 June 2021, Frank Peterson v. Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH and Elsevier Inc. v. Cyando AG, Joined Cases C-682/18 and 683/18, ECLI:EU:C:2021:503, 114.

30 As one commentator pointed out, "even though key principles might endure, the transformation of the context is too drastic and substantial to simply force adaptation of existing rules." See: Teresa Rodríguez de las Heras Ballell, "The Background of the Digital Services Act: Looking Towards a Platform Economy," *ERA Forum* 22, (2021): 78, https://link.springer.com/article/10.1007/s12027-021-00654-w.

31 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Tackling Illegal Content Online. Towards an Enhanced Responsibility of Online Platforms*, Brussels, 28 September 2017, COM(2017) 555 final.

voluntary arrangements. As a follow-up on that Communication, the Commission Recommendation of 2018 on measures to effectively tackle illegal content online acknowledged that illegal content online remains a serious problem within the European Union despite the progress that had been made through voluntary arrangements of various kinds and encouraged Member States and hosting service providers to take effective, appropriate, and proportionate measures to tackle illegal content online.[32]

The succession of social media-related scandals that followed the Cambridge Analytica affair proved that self-regulatory efforts of platforms against online harms had not been efficient.[33] Some Member States adopted their own regulations targeting specific online harms, which again raised concerns about the risk of fragmentation of intermediary regulation within the European Union.[34] The European Commission decided to intervene. In early 2020 the Commission made a commitment to update the horizontal rules that define the responsibilities and obligations of providers of digital services,[35] and on December 15, 2020 published a proposal for a Digital Services Act.[36] After a political consensus was reached, the final text was adopted on October 19, 2022.[37]

---

32 European Commission, Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, C/2018/1177 (O.J.E.C. L63, 6 March 2018), 50–61, accessed June 4, 2024, https://eur-lex.europa.eu/eli/reco/2018/334/oj.

33 Amelie P. Heldt, "EU Digital Services Act: The White Hope of Intermediary Regulation," in *Digital Platform Regulation. Global Perspectives on Internet Governance*, eds. Terry Flew and Fiona R. Martin (Cham: Palgrave Macmillan, 2022), 70, accessed June 4, 2024, https://link.springer.com/chapter/10.1007/978-3-030-95220–4_4.

34 Matthias Cornils, *Designing Platform Governance: A Normative Perspective on Needs, Strategies, and Tools to Regulate Intermediaries*, Governing Platforms (Algorithm Watch, May 2020), 77, accessed June 4, 2024, https://algorithmwatch.org/de/wp-content/uploads/2020/05/Governing-Platforms-legal-study-Cornils-May-2020-AlgorithmWatch.pdf.

35 European Commission, Communication: Shaping Europe's Digital Future, 19 February 2020, COM/2020/67 final, accessed June 6, 2024, https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf.

36 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, Brussels, 15 December 2020, COM(2020) 825 final.

37 Regulation (EU) No. 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a digital single market for services and amending Directive 2000/31/EC (Digital Services Regulation) (O.J.E.C. L277, 27 October 2022), Document L: 2022:277:TOC, accessed June 6, 2024, https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

3. Online Platforms: A New Player in the European Union Legal Order

Unlike the ECD and contrary to what its name suggests, the DSA does not regulate all digital services (or "information society services" in the terminology of the ECD),[38] only the "intermediary services."

The DSA's scope of application is thus narrower than that of the ECD. However, as far as the regulation of intermediation services is concerned, the DSA is much more ambitious since it does not merely reproduce the liability exemption provisions already enshrined in the ECD, but it also contains rules on specific due diligence obligations tailored to certain specific categories of intermediary services and on the implementation and enforcement of these obligations. This is consistent with the goal of the new standard, which is to create a safe, predictable, and trusted online environment for intermediary services in order to both contribute to the proper functioning of the internal market and facilitate innovation and also ensure that fundamental rights, including consumer protection, are effectively protected.[39]

The notion of intermediary service providers is not new but comes from the ECD. As opposed to content providers, intermediary service providers are digital services that transmit or store content that a third party has provided. Like the ECD, the DSA does not provide a definition of intermediary services but merely describes the services that fall into this category, namely conduit, caching, and hosting.[40] Firstly, mere conduit services provide access to a communication network or transmit the information provided by users, including Internet access, wireless access points, virtual private networks, DNS services and resolvers, IP telephony, or instant

[38] The definition of "information society service" may be found in Article 1(1)(b) of Directive (EU) No. 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (O.J.E.C. L241, 17 September 2015), 1–15, accessed June 6, 2024, https://eur-lex.europa.eu/eli/dir/2015/1535/oj. According to this provision, an information society service is any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. Within this broad definition, two categories of information society service providers can be distinguished, content providers and intermediary providers.

[39] Article 1(1) DSA.

[40] Article 3(g) DSA.

messaging. Caching services are also related to the transmission of information provided by a recipient of the service in a communication network, but it involves the automatic, intermediate, and temporary storage of that information for the sole purpose of making the information's onward transmission to other recipients more efficient upon their request. Such services are crucial to ensure the smooth and efficient transmission of information delivered on the Internet. Finally, hosting services consist of the storage of the information supplied by the service recipient. Typical examples are web hosting and cloud service providers.

However, the DSA introduces new subcategories that did not appear in the ECD. First and foremost, Article 3(i) defines "online platforms" as a subcategory of hosting service providers characterized by the fact that they do not only store data at the request of the recipient of the service but also disseminate this information to the public, as is the case with social networks, online marketplaces, app stores, or content-sharing providers.

Moreover, the DSA identifies a specific subcategory of online platforms that are likely, due to their size, to have a greater impact on the dissemination of illegal or harmful content, the propagation of fake news, incitement to hatred, etc. These are known as "very large online platforms" (VLOPs), subject to additional due diligence obligations that overlap with those imposed on other online platforms. The threshold for an online platform to be considered "very large" is to have a number of average monthly active users in the Union equal to or higher than 45 million, a number roughly corresponding to 10 % of the Union population.[41]

Finally, the DSA extends the specific obligations of VLOPs to "very large online search engines" (VLOSEs). This category was not included in the Proposal of the Commission and does not fit very well with the overall structure of the DSA.[42] They are considered intermediary services,[43] but they are not listed in Article 3(g), along with mere conduit, proxy caching, or hosting services, nor are they included in Chapter II on the liability of providers of intermediary services.

41 Article 33 and recital 76 DSA.

42 Folkert Wilman, "The Digital Services Act (DSA): An Overview," December 2022, 4, https://ssrn.com/abstract=4304586.

43 See Article 3(j) DSA.

4. What Remains and What Is New in the DSA Liability Regime

With regard to the liability exemption regime, Articles 5–7 DSA virtually reproduce the wording of Articles 12–14 ECD, as does Article 8 DSA, prohibiting imposing a general monitoring obligation previously enshrined in Article 15 ECD. The aforementioned provisions of the ECD are repealed and replaced by their equivalents in the DSA,[44] which is more relevant than it might seem. Indeed, although, in essence, the liability exemption rules have not changed, the normative instrument in which they are now contained is no longer a directive but a regulation with direct effect in all Member States. This should resolve the numerous issues arising from the varying implementations of the ECD by the Member States.[45]

Apart from reproducing the pre-existing liability exemptions for the different categories of ISPs, the DSA contains some clarifications and adds new features to the liability regime of intermediary service providers.[46]

First, the DSA codifies the neutrality requirement for intermediary service providers to benefit from the liability exemptions. However, as one commentator has sharply observed, there seems to be a slight variation from previous case law since the reference to neutrality is not dependent on the intermediary's merely passive role.[47] In this regard, recital 18 DSA clarifies that

> the exemptions from liability should not apply where, instead of confining itself to providing the services neutrally by a merely *technical and automatic* processing of the information provided by the recipient of the service,

[44] Article 89(1) DSA. Therefore, references to Articles 12 to 15 ECD is construed as references to Articles 4, 5, 6 and 8 DSA, respectively.

[45] However, as some commentators have pointed out, this does not entirely exclude the risk of fragmentation and uncertainty since the DSA does not provide a positive basis for establishing when a provider can be held liable, which will still be determined by national law (recital 17 DSA). See: Aina Turillazzi et al., "The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications," January 12, 2022, 9–11, https://ssrn.com/abstract=4007389.

[46] Pursuant to Recital 16, the DSA seeks to preserve the intermediary liability framework of the ECD and clarify certain elements of that framework with regard to the case law of the Court of Justice of the European Union. A closer look reveals that the new regulation also incorporates some novelties that had no precedent either in the ECD or in previous decisions of the CJEU.

[47] Wilman, "The Digital Services Act," 5.

> the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information.[48]

A service provider may thus benefit from the liability exemption regime even if it has been active to a certain extent as long as it does not lead to knowledge or control over the illegal content. As we discussed above, this was already the interpretation adopted by the Court of Justice, but the references to the passive role of the intermediary made in some cases by the Court could be misleading.

A second important clarification is found in Article 7, which contains what is known as *the Good Samaritan clause* inspired by section 230 CDA. A question that has always haunted ISPs is whether taking proactive steps to moderate illegal content rather than merely responding to take-down notices would be understood as taking control of the information they host and consequently becoming liable for unlawful content supplied by third parties.[49] This would send a dangerous message for a safe digital environment since it could discourage intermediaries from carrying out activities that aim to detect, identify, and act against illegal content on a voluntary basis.[50] Confirming the interpretation of the Court of Justice[51]

---

48 Emphasis added to point out that the reference to the passivity of the service provider that appeared in recital 42 ECD has been dropped.

49 The Prodigy case, considered the driving factor for the US Congress to pass section 230 CDA, is a good example. The New York State Supreme Court concluded that a service provider qualified as a publisher of defamatory content hosted on a forum because it exercised some control over the comments posted by users on its website insofar as it used software to detect offensive terms and had moderators who removed inappropriate comments [Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995)].

50 European Commission, Staff working document, *Impact Assessment Accompanying the 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*, Brussels, 15 December 2020, SWD(2020) 348 final, Part 1/2, 24–5.

51 See: CJEU Judgment of 22 June 2021, Frank Peterson v. Google LLC and Others, and Elsevier Inc. v. Cyando AG, Joined Cases C-682/18 and 683/18, ECLI:EU:C:2021:503, 109, where the Court of Justice concluded that only because the operator of a video-sharing platform (YouTube) implements technological measures aimed at detecting content which may infringe copyright, it does not mean that operator plays an active role giving it knowledge of and control over the content of those videos.

and the European Commission,[52] Article 7 DSA clarifies now that the mere fact that providers undertake voluntary, proactive measures to fight against illegal content does not automatically render unavailable the exemptions from liability, provided those activities are carried out in good faith and a diligent manner.

Like the ECD, the DSA clarifies that the exemption from liability does not affect the possibility that courts or administrative authorities require intermediary service providers to terminate or prevent infringements committed by their users. However, Article 9 DSA further elaborates and harmonizes certain information that such orders have to contain, such as the legal basis for the order, a statement of reasons explaining why the information is illegal content, the identification of the issuing authority, and clear information enabling the provider of intermediary services to identify and locate the illegal content concerned. Similarly, Article 10 DSA contains the conditions to be met by orders that relevant national authorities might issue to request specific information about the recipients of intermediary services.

One of the key novelties of the DSA is the obligation for hosting service providers to implement a notice-and-action procedure, which is meant to facilitate that any person concerned by a specific item of information that they consider to be illegal can report to the hosting provider (notification) so that the later can remove or disable access to such content (action). This notice and action mechanism is closely connected with the liability exemption regime of hosting service providers since notifications that meet the conditions laid down by the law will be considered to give rise to actual knowledge or awareness for the purposes of Article 6 DSA in respect of the specific item of information reported where they allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination.[53]

---

52 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Tackling Illegal Content Online. Towards an Enhanced Responsibility of Online Platforms*, Brussels, 28 September 2017, COM(2017) 555 final, 10; after suggesting that in light of their central role and capabilities and their associated responsibilities, online platforms should adopt effective proactive measures to detect and remove illegal content and not only limit themselves to reacting to notices received.

53 Article 16(3) DSA.

The requirement that the illegality of the information is manifest, without the need for an individualized assessment by the service provider, had already been established by courts.[54] Indeed, the notification by the concerned party may prove that the provider is aware of the existence of a certain piece of information hosted in its servers, but this is not sufficient to exclude the application of the liability exemption set out in Article 6 DSA because it is one thing to be aware of the existence of certain content and quite another to have actual knowledge that this content is illegal. This may be the case if there is a prior decision by a competent body declaring the illegality. Otherwise, it is not sufficient to inform the provider of the presence of the allegedly unlawful content, but the illegality of such content must be self-evident without the service provider having to carry out a complex legal assessment to determine the illegality of the content. For example, intermediary service providers would not bear the burden of assessing whether the content is illegal when the alleged illegality consists in the falsehood of the information or when fundamental rights such as the right to honor and freedom of expression come into conflict, which would require a complex balancing exercise.

The DSA also contains a specific provision for a subcategory of hosting providers, namely online marketplaces that allow consumers to conclude a distance contract, like Amazon or eBay. According to Article 6(1) DSA, these platforms should not benefit from the general liability exemption for hosting service providers with respect to liability arising from consumer protection rules, where such online platforms present the relevant information relating to the transactions at issue in such a way as to lead an average consumer to believe that the information, product, or service is provided by the online platforms itself or by traders acting under their authority or

[54] See: CJEU Judgment of 3 October 2019, Eva Glawischnig-Piesczek v. Facebook Ireland Limited, Case C-18/18, ECLI:EU:C:2019:821, 45, which considers that if the hosting provider were required to make an "autonomous assessment" in order to determine the illegality of the content at issue, this would amount to a general monitoring obligation, prohibited by Article 15 ECD; ECtHR Judgment of 2 February 2016, Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, application no. 22947/13, 64, distinguishing the case at issue from Delfi [ECtHR Judgment of 16 June 2015, Delfi As v. Estonia, application no. 64569/09)] on the grounds that the incriminated comments could be considered offensive and vulgar but did not constitute "clearly unlawful speech," nor certainly amount to hate speech or incitement to violence.

control, so that the platform has knowledge of or control over the information, even if that may in reality not be the case. An example would be when an online platform markets the product or service in its own name rather than in the name of the trader who will supply that product or service or when the platform only reveals the identity or contact details of the trader once the contract between the trader and the consumer has been concluded.[55] This provision aims to ensure the effective protection of consumers when engaging in intermediated commercial transactions online.

5. With Great Power Comes Great Responsibility: Obligations for Online Platforms Under the DSA

The DSA goes far beyond the liability exemptions regime under the ECD. After more than 20 years, the digital landscape has drastically changed. Online activities are an important part of our lives, ranging from connecting to friends and family, accessing information, cultural products, or educational content to the performance of all kinds of contracts. New and innovative business models and services have emerged, creating new risks and challenges for individuals, companies trading online, and society as a whole. Accordingly, the aim of the DSA is not only to contribute to the proper functioning of the internal market for intermediary services and to facilitate innovation but also to set out harmonized rules for a safe, predictable, and trusted online environment in which fundamental rights enshrined in the Charter, including consumer protection, are effectively protected.[56] To achieve this goal, providers of intermediary services must behave responsibly and diligently,[57] which explains why a big part of the DSA deals with due diligence obligations for intermediary service providers.[58]

As we have already seen, the DSA differentiates one kind of provider of intermediary services from another by their type, the nature of the service

55 Recital 24 DSA.

56 Article 1(1) DSA.

57 Recital 3 DSA. As a commentator nicely put it, the DSA has chosen a "procedure before substance" approach, creating a series of procedural obligations and redress avenues rather than setting forth any bright-line substantive rule on the limits of online freedom of expression; Pietro Ortolani, "If You Build It, They Will Come The DSA's 'Procedure Before Substance' Approach," Verfassungsblog, November 7, 2022, accessed June 4, 2024, https://verfassungsblog.de/dsa-build-it/.

58 Chapter III, Articles 11–48 DSA.

they provide, and their size. Based on the resulting categories, the new regulation designs an "asymmetric" system of due diligence obligations.[59] General obligations, such as the designation of a single point of contact to enable communication with authorities and a legal representative when they do not have an establishment in the European Union, apply to all intermediary service providers, including mere conduit, proxy caching, and hosting providers.[60]

A second layer of due diligence obligations is tailored to hosting service providers based on their potential role in tackling illegal content online.[61] Regardless of their size, hosting providers must put in place easily accessible and user-friendly notice and action mechanisms. They are also required to provide a clear and specific statement of reasons when they impose restrictions because the information provided by the service recipient is illegal or incompatible with their terms and conditions. Moreover, providers of hosting services are required to promptly inform the competent national law enforcement or judicial authorities if they become aware of any information giving rise to a suspicion of certain serious criminal offences.

A number of additional obligations address, in particular, online platforms, such as social networks, content-sharing platforms, app stores, online marketplaces, and online travel and accommodation platforms.[62] For instance, providers of these services are required to set up an internal redress mechanism to handle complaints against any decision they make on the grounds that the information provided by the recipients is illegal or

---

59 Due diligence obligations under the DSA apply in a cumulative manner to those intermediary services that fall within a number of different categories. For instance, the provider of an online platform must not only comply with the specific obligations foreseen for online platforms but also with those for hosting services and intermediary services in general. See: Recital 41 DSA.

60 Articles 11–15 DSA.

61 Articles 16–18 DSA.

62 Articles 20–29 DSA. However, with regard to obligations imposed on online platforms, Article 19 DSA makes an important caveat: they do not apply to providers that qualify as micro or small enterprises, that is, enterprises which employ fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million. This cap is included to avoid disproportionate burdens on relatively small providers of online platforms (Recital 57 DSA), which in turn responds to the goal of encouraging innovation and promoting the entry of newcomers to the platform economy.

incompatible with the terms and conditions of the platform.[63] Other obligations imposed on online platforms may have a direct impact on certain common business practices, such as the prohibition of designing, organizing, or operating their online interfaces (i.e. website or apps)[64] in a way that misleads or manipulates users or that materially distorts or impairs users' ability to make free and informed decisions. These practices, known as "dark patterns," include design choices to direct users to make decisions that are not beneficial for them but for the provider of the online platform, presenting choices in a non-neutral manner, repeatedly requesting a recipient of the service to make a choice where such a choice has already been made, making the procedure of cancelling a service significantly more cumbersome than signing up to it or making certain decisions more difficult or time-consuming than others.[65] Transparency obligations imposed on online platforms are also particularly intense, affecting how they present advertisements on their online interfaces to their recommender systems.[66]

In addition, those online platforms allowing consumers to conclude distance contracts with traders must comply with specific obligations.[67] To begin with, providers of B2C online marketplaces have to obtain certain specific information from traders and make "reasonable efforts" to verify the reliability of the information submitted ("know your business customer obligation"). Besides, they have to design their online interfaces to enable traders to comply with their obligations regarding pre-contractual information, compliance, and product safety information. Finally, if the provider of an online platform becomes aware that a trader has offered an illegal product or service through its service, it has to inform the consumers who purchased the unlawful product or service.

The more demanding obligations concern very large online platforms (VLOPs), which are considered to have a significant societal and economic

63 On this issue, see: Sebastian Kuclar Stiković, "The EU's Digital Services Act and Its Impact on Online Platforms," *European Union Law Working Papers*, no. 84 (2024): 55, accessed June 4, 2024, https://law.stanford.edu/wp-content/uploads/2024/02/EU-Law-WP-85-Stikovic.pdf. This author argues that the lack of detail in the regulation of the redress mechanism may prove detrimental to ensure effective access to justice.

64 Article 3(m) DSA.

65 Recital 67 DSA.

66 Articles 26–27 DSA.

67 Articles 30–32 DSA.

impact and therefore bear more responsibility in curbing illegal content online.[68] Once designated as such, these entities are required to carry out a yearly self-assessment of systemic risks caused by the design or the functioning of their services, including the dissemination of illegal content, any negative effect on the exercise of fundamental rights, or any actual or foreseeable negative effects on civic discourse and electoral processes. When systemic risks are identified, VLOPs must put in place reasonable, proportionate, and effective mitigation measures that may affect, inter alia, their online interfaces, terms and conditions, content moderation processes, or algorithmic systems, including their recommender systems. Moreover, compliance with these obligations and any commitments undertaken under codes of conduct or crisis protocols have to be audited at least once a year by independent private firms. In addition, VLOPs are also subject to additional transparency reporting obligations and have to provide data access for legal authorities and researchers.

In order to ensure that due diligence obligations are fulfilled, the DSA contains an extensive set of provisions on supervision and enforcement by national and EU authorities, which is reinforced by the possibility of imposing penalties, including financial fines, that amount up to 6% of the global turnover of a service provider for the case of VLOPs and VLOSEs.[69] Therefore, it can be argued that providers of intermediary services are exempted from liability for the content transmitted or hosted by their users as long as they comply with the requirements of the safe harbor provisions, but now they may also be held liable if they fail to comply with the due diligence obligations imposed by the DSA.

6. Territorial Scope of the DSA and the So-Called "Brussels Effect"

The DSA is likely to have a major impact even beyond the borders of the European Union.[70] This may happen in two different ways. Firstly, since the regulatory problems faced by the DSA are universal, lawmakers around

68 Articles 33–43 DSA.

69 Articles 49–88 DSA.

70 Daphne Keller, "The EU's new Digital Services Act and the Rest of the World," Verfassungsblog, November 7, 2022, accessed June 4, 2024, https://verfassungsblog.de/dsa-rest-of-world/. This author argues that some effects of the DSA will be positive and probably lead to real benefits for users, but others may be problematic.

the world might be tempted to adopt their own platform regulations along the lines of the European model, especially in developing countries that do not have the regulatory expertise of the European Union.[71] Secondly, digital companies operating globally will likely extend compliance measures meant for the European Union to all their customers regardless of the country in which they are based, thus making the DSA rules the de facto standard.[72] This phenomenon, known as "the Brussels effect," has already some precedents in other areas of law.[73]

The spillover effect of the DSA in the rest of the world is partly a consequence of its broad scope of application. Needless to say, the DSA is only enforceable in the European Union, where, as a regulation, it applies directly without the need for transposition into national law by the Member States. However, its scope is not limited to service providers who have their place of establishment or are located in the European Union but under Article 2(1) DSA applies to all intermediary service providers who offer their services to users who have their place of establishment or are located in the European Union. In other words, the DSA applies to intermediary service providers irrespective of their place of establishment or location so far as they offer services in the Union. In order to determine whether an operator offers its services in the European Union, it will be necessary to assess whether there is a "substantial connection" with the Union.[74] Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union or, in the absence of such an establishment, where the number of recipients of the service in one

71 Anu Bradford, "The European Union in a Globalised World: The 'Brussels Effect'," *Groupe d'études géopolitiques*, no. 2 (2021): 75; Zingales Nicolo, "The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence: Hail to Meta-Regulation," Verfassungsblog, November 2, 2022, accessed June 4, 2024, https://verfassungsblog.de/dsa-meta-regulation/.

72 Some author suggests that the European Union could also promote the DSA as a global model, incorporating parts of it into its model free trade agreements. See: Anupam Chander, "When the Digital Services Act Goes Global," *Berkeley Technology Law Review* 38, no. 3 (2023): 1072–3.

73 The phrase "Brussels effect" was first coined by Anu Bradford in 2012 to describe the growing role that the EU plays in imposing standards that multinational companies voluntarily extend to govern their global operations, see: Anu Bradford, "The Brussel Effect," *Northwestern University Law Review* 107, no. 1 (2012): 1–68.

74 Recital 7 DSA.

or more Member States is significant in relation to the population thereof, or based on the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States can be determined considering all relevant circumstances, such as the use of a language or a currency generally used in that Member State, the use of a relevant top-level domain, or the provision of local advertising, to name a few.[75] In contrast, just because a website is accessible from the European Union is not enough for it to be considered a substantial connection to the Union.

Presumably, if platforms are obliged to make some changes to comply with the strict requirements of the DSA, they will likely extend these benefits in other countries where they operate since it is not economically, legally, or technically practical to maintain lower standards in non-EU markets. For instance, more clearly articulated terms and conditions under Article 14 DSA or the explanation of their recommender systems under Article 27 DSA will improve transparency both inside and outside the European Union. The same logic applies to many other provisions of the DSA.

References

Barceló, Rosa Julià. "Liability for On-line Intermediaries. A European Perspective." *E.I.P.R.*, no. 12 (1998): 453–63.

Bradford, Anu. "The Brussel Effect." *Northwestern University Law Review* 107, no. 1 (2012): 1–68.

Bradford, Anu. "The European Union in a Globalised World: The 'Brussels Effect'." *Groupe d'études géopolitiques*, no. 2 (2021): 75–9.

Chander, Anupam. "When the Digital Services Act Goes Global." *Berkeley Technology Law Review* 38, no. 3 (2023): 1067–88.

Cornils, Matthias. *Designing Platform Governance: A Normative Perspective on Neeeds, Strategies, and Tools to Regulate Intermediaries*. Governing Platforms. Algorithm Watch, May 2020. Accessed June 4, 2024. https://algorithmwatch.org/de/wp-content/uploads/2020/05/Governing-Platforms-legal-study-Cornils-May-2020-AlgorithmWatch.pdf.

Crabit, Emmanuel. "La directive sur le commerce éléctronique." *Revue du Droit de l'Union Européenne*, no. 4 (2000): 749–833.

van Eecke, Patrick. "Online Service Providers and Liability: A Plea for a Balanced Approach." *Common Market Law Review* 48, no. 5 (2011): 1455–502.

[75] Recital 8 DSA.

Edwards, Lilian. "'With Great Power Comes Great Responsibility?': The Rise of Platform Liability." In *Law, Policy and the Internet*, edited by Lilian Edwards, 253–89. Oxford: Hart, 2019.

Elkin-Koren, Niva. "Fair Use by Design." *UCLA Law Review* 66, (2017): 1082–100.

Heldt, Amelie P. "EU Digital Services Act: The White Hope of Intermediary Regulation." In *Digital Platform Regulation. Global Perspectives on Internet Governance*, edited by Terry Flew and Fiona R. Martin, 69–84. Cham: Palgrave Macmillan, 2022. Accessed 2024–06–04. https://link.springer.com/chapter/10.1007/978-3-030-95220–4_4.

Johnson, Neville L., Douglas L. Johnson, Paul Tweed, and Rodney A. Smolla. "Defamation and Invasion of Privacy in the Internet Age." *Southwestern Journal of International Law* 25, no. 1 (2019): 9–41.

Keller, Daphne. "The EU's new Digital Services Act and the Rest of the World." Verfassungsblog, November 7, 2022. Accessed June 4, 2024. https://verfassungsblog.de/dsa-rest-of-world/.

Kosseff, Jeff. *The Twenty-Six Words That Created the Internet.* Ithaca, London: Cornell University Press, 2019.

Lemarchand, Stéphane, and Marion Barbier. "Le fournisseur d'hébergement au sens de l'article 14 de la directive 2000/31 e la (nouvelle?) condition de neutralité." *Revue Lamy Droit de l'Immatériel*, no. 54 (2009): 52–6.

Ortolani, Pietro. "If You Build It, They Will Come The DSA's 'Procedure Before Substance' Approach." Verfassungsblog, November 7, 2022. Accessed June 4, 2024. https://verfassungsblog.de/dsa-build-it/.

Peguera Poch, Miquel. "The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems." *Colum. J. L. & Arts* 32, (2009): 481–512.

Rodríguez de las Heras Ballell, Teresa. "The Background of the Digital Services Act: Looking Towards a Platform Economy." *ERA Forum* 22, (2021): 75–86. https://doi.org/10.1007/s12027-021-00654-w.

Sartor, Giovanni. "Providers Liability: From the eCommerce Directive to the Future. In-Depth Analysis for the IMCO Committee," October 2017. Accessed June 4, 2024. https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf.

Stalla-Bourdillon, Sophie. "Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well." In *The Responsibilities of Online Service Providers*, edited by Mariarosaria Taddeo and Luciano Floridi, 275–93. Cham: Springer, 2017.

Stiković, Sebastian Kuclar. "The EU's Digital Services Act and Its Impact on Online Platforms." *European Union Law Working Papers*, no. 84 (2024). Accessed

June 4, 2024. https://law.stanford.edu/wp-content/uploads/2024/02/EU-Law-WP-85-Stikovic.pdf.

Synodinou, Tatiana-Eleni. "Intermediaries' Liability for Online Copyright Infringement in the EU: Evolutions and Confusions." *Computer Law & Security Review* 31, (2015): 72–96.

Turillazzi, Aina, Federico Casolari, Mariarosaria Taddeo, and Luciano Floridi. "The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications," January 12, 2022. https://ssrn.com/abstract=4007389.

Walden, Ian. "Mine Host Is Searching for a 'Neutrality' Principle!." *Computer Law & Security Review* 26, no. 2 (2010): 203–9.

Wilman, Folkert. "The Digital Services Act (DSA): An Overview," December 2022. https://ssrn.com/abstract=4304586.

Zingales, Nicolo. "The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence: Hail to Meta-Regulation." Verfassungsblog, November 2, 2022. Accessed June 4, 2024. https://verfassungsblog.de/dsa-meta-regulation/.