3

Platform Responsibility in the European Union

From the E-Commerce Directive to the Digital Services Act

Christoph Busch

On February 17, 2024, the Digital Services Act (DSA) became fully applicable in the European Union (EU). The DSA, which has been portrayed as Europe's new "Digital Constitution," sets out a cross-sector regulatory framework for online services and regulates the responsibility of online intermediaries for illegal content. Against this background, this chapter provides a brief overview of recent regulatory developments regarding platform responsibility in the EU. The chapter forms part of the volume's comparative research project focused on inconsistencies among jurisdictions, the international effects of national structures for responsibility, and the possibility of international coordination of reform. In this context, the chapter seeks to add a European perspective to the global debate about platform regulation. Section 3.1 provides an overview of the regulatory framework in the EU and recent legislative developments. Section 3.2 analyzes different approaches regarding the enforcement of rules on platform responsibility. Section 3.3 takes a closer look at the regulation of content moderation by digital platforms in the EU. Finally, Section 3.4 adds some observations on the international effects of EU rules on platform responsibility.

3.1 GENERAL OVERVIEW ON PLATFORM RESPONSIBILITY

Platform responsibility in the EU is based on a combination of horizontal and sector-specific rules. For more than twenty years, the central pillar of the regulatory framework for digital services at EU level has been the E-Commerce Directive[1] (ECD).[2] Over the past few years, it has been complemented by sector-specific regulatory initiatives (Section 2). Furthermore, several Member States have recently

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), http://data.europa.eu/eli/dir/2000/31/oj (hereinafter *ECD*).

[2] *See* Alexandre de Streel and Martin Husovec, The e-commerce Directive as the cornerstone of the Internal Market: Assessment and options for reform, Study for the IMCO committee of the

enacted national laws imposing responsibility on platforms in specific subject areas (Section 3). With the proposal for a Digital Services Act (DSA),[3] published in December 2020, the European legislator has taken an important step toward a comprehensive reform of the regulatory framework for platform responsibility (Section 4). A political agreement[4] on the outline of the DSA was reached in April 2022 and the DSA was formally adopted in October 2022.[5]

3.1.1 *The E-Commerce Directive*

The ECD, which laid the foundations for the EU regulatory framework for digital services, did not provide a positive basis for establishing when a provider of online services can be held liable for illegal content online. Instead, it created a horizontal framework of conditional exemptions from liability for different types of online service providers.[6] For hosting providers, including online platforms, legal immunity was based on a knowledge standard. Unlike Section 230 of the US Communications Decency Act,[7] which gives absolute immunity to publishers (other than immunity from Federal criminal law and certain intellectual property and sex trafficking claims), the ECD shielded platforms from liability only if they did not know that they are hosting illegal content. Under Art. 14 ECD, a platform operator was not liable for information stored at the request of a user, subject to the satisfaction of two alternative conditions. First, if "the provider does not have actual knowledge of illegal activity or illegal content."[8] Second, if "the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the illegal content."[9] According to well-established case law of the European Court of Justice, the applicability of these safe harbor provisions depends on whether the intermediary has played a "neutral role" or an "active role."[10] In the cases *Google France v. Louis Vuitton*[11] and *L'Oreal v. eBay*,[12] the European Court of

European Parliament (May 2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648797/IPOL_STU(2020)648797_EN.pdf.

3 European Commission, Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM (2020) 825 final (hereinafter *DSA Proposal*).

4 DSA, Provisional Agreement (Apr. 23, 2022). The text of the provisional agreement is available here: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/DV/2022/06-15/DSA_2020_0361COD_EN.pdf (hereinafter *DSA Provisional Agreement*).

5 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, http://data.europa.eu/eli/reg/2022/2065/oj (hereinafter *DSA*).

6 *See* Arno R. Lodder & Andrew D. Murray, EU Regulation of E-Commerce 47–54 (2017).

7 47 U.S.C. § 230.

8 *See* ECD, *supra* note 1, art. 14(1)(a).

9 *See* ECD, *supra* note 1, art. 14(1)(b).

10 *See also* ECD, *supra* note 1, Recital 42.

11 CJEU Case C-236/08, Google France v. Louis Vuitton, ECLI:EU:C:2010:159 (Mar. 23, 2010).

12 CJEU Case C-324/09, L'Oreal v. eBay, ECLI:EU:C:2011:474 (July 12, 2011).

Justice has stated that the liability exemptions do not apply to service providers who play an active role, which would give the provider knowledge or control over the activity or information that is hosted. The safe harbor rule is complemented by Art. 15 ECD, which underlines that platform operators have no general obligation to monitor information on the platform.

3.1.2 *Sector-Specific Legislation and Self-regulation at EU Level*

In the light of the dynamic development of the digital economy over the past two decades, it became evident that the ECD in its present state no longer provides an adequate regulatory framework for the emerging "platform society."[13] In response to the rise of large online platforms, the EU has adopted over the past few years a variety of regulatory initiatives, including sector-specific legislation and measures based on self-regulation. These initiatives, which were meant to complement the ECD, seek to provide a regulatory response to the increasingly complex digital environment and the dissemination of illegal and harmful content.[14] Some of them focus on specific services (e.g., audiovisual media services),[15] others address specific types of illegal content (e.g., illegal hate speech,[16] terrorist content).[17] Others again tackle the dissemination of content that is harmful, but not necessarily illegal (e.g., online disinformation).[18] This piecemeal approach added to the fragmentation of the regulatory landscape and failed to provide a comprehensive update of the ECD, in particular in terms of responsibilities and regulatory oversight.[19] A few examples may illustrate this sector-specific approach.

Hate speech. Regarding illegal hate speech, the EU opted for self-regulation by platforms. Thus, in May 2016, the European Commission published the EU Code

[13] *See* José van Dijck, Thomas Poell & Martijn de Waal, The Platform Society: Public Values in a Connective World (2018).

[14] Ilaria Buri and Joris van Hoboken, *The Digital Services Act (DSA) Proposal: A Critical Overview* 5 (DSA Observatory, Oct. 28, 2021), https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf.

[15] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, 2018 O.J. (L 303) 69–92 (hereinafter *AVMS Directive*).

[16] European Commission, *The EU Code of conduct on countering illegal hate speech online* (June 30, 2016), https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en#theeucodeofconduct.

[17] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, 2021 O.J. (L 172) 79–109 (hereinafter *TCO Regulation*)

[18] European Commission, *EU Code of Practice on Disinformation* (2018), https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

[19] Buri and Hoboken, *supra* note 14, at 8.

of Conduct on Countering Illegal Hate Speech Online.[20] Initial signatories of the Code of Conduct included Facebook, Microsoft, Twitter, and YouTube. Today, the list of signatories also includes TikTok, LinkedIn, Twitch, and other platforms.[21] Considering that there is no formal definition of "hate speech" in International Human Rights Law, the Code of Conduct, adherence to which is voluntary, builds on the definition of illegal hate speech adopted by the Council of the European Union.[22] Under the Code of Conduct, the signatories made several voluntary commitments to counter the spread of illegal hate speech. In particular, they committed themselves to put in place mechanisms that allow them to review the majority of notifications on illegal content submitted by users within twenty-four hours and remove or disable access to such content, if necessary. In addition, platforms pledged to intensify cooperation between themselves and other platforms and social media companies to enhance best practice sharing. The implementation of the Code is evaluated through regular monitoring rounds. The performance reports are published by the European Commission.[23]

Disinformation. Another subject area, where the EU has promoted platform self-regulation, is the fight against disinformation. In September 2018, the European Commission released the Code of Practice on Disinformation,[24] under which the signatories (including Facebook, Google, Twitter, TikTok, and several advertising industry associations) voluntarily commit to take measures to minimize the spread of online disinformation. In order to coordinate these efforts, the Code of Practice contains a wide range of commitments: from transparency requirements for political advertising, to the termination of fake accounts, to the demonetization of disinformation campaigns.

Following a revision process launched in 2021, a revised and strengthened Code of Practice was released in June 2022 by the European Commission. It is planned that the new Code of Practice shall become part of a broader regulatory framework in combination with the future DSA. In particular, for very large platforms (VLOPs)[25] and very large search engines (VLOSEs)[26] with at least forty-five million

[20] European Commission, *supra* note 16.

[21] *Id.*

[22] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, 2008 O.J. (L 328), (defining illegal hate speech as "all conduct publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, color, religion, descent or national or ethnic origin").

[23] European Commission, *supra* note 16.

[24] EU Code of Practice on Disinformation, *supra* note 18. In May 2023, the social media platform X (formerly Twitter) announced its intention to exit the voluntary Code, *see* Luca Bertuzzi, *Twitter Set to Exit EU Code of Practice on Disinformation, Sources Say*, EURACTIV (May 26, 2023), https://www.euractiv.com/section/digital/news/twitter-set-to-exit-eu-code-of-practice-on-disinformation-sources-say/.

[25] DSA, *supra* note 5, art. 33.

[26] *Id.* art. 33a.

average monthly active users, adherence to the Code of Practice will constitute a risk mitigation measure required under Art. 27 DSA. In 2023, the EU adopted two series of designation decisions under the DSA designating twenty VLOPs and two VLOSEs.[27] Following their designation, the companies will have to comply with the full set of new obligations under the DSA. The examples above show that the DSA will not entirely replace the existing regulatory instruments but rather incorporate them into a more comprehensive governance framework that combines horizontal and sector-specific rules, as well as binding and non-binding instruments.

Terrorist content. The controversial EU Regulation on addressing the dissemination of terrorist content online (TCO Regulation),[28] which came into force in June 2021, establishes uniform rules to address the misuse of hosting services for the dissemination to the public of terrorist content online, which have direct effect across the EU as of June 7, 2022. Under the TCO Regulation, hosting service providers, including social media platforms, video-sharing services, and cloud services, may be required to remove flagged "terrorist content"[29] across the entire EU within specific time frames.

Notably, national authorities have the power to issue "removal orders" requiring hosting service providers to remove or disable access to terrorist content in all EU Member States "as soon as possible and, in any event, within one hour of receipt of the removal order."[30] In addition, the TCO Regulation includes a number of measures to ensure transparency, accountability, and the protection of legal rights. For example, platforms will have the right to challenge a removal order in court.[31] Furthermore, they must put in place complaint-handling mechanisms that allow users whose content has been removed to request a reinstatement of the content.[32]

When the DSA entered into force, it did not replace the TCO Regulation. Instead, the DSA explicitly mentions the TCO Regulation in the list of sector-specific legislation that will continue to apply as *lex specialis*.[33] The same applies to

[27] The first set of VLOPs, designated in April 2023, includes Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, and Zalando. The second set of VLOPs, designated in December 2023, includes three platforms that host sexually explicit content: Pornhub, Stripchat, and XVideos. In addition, in April 2023, the European Commission designated two VLOSEs: Bing and Google Search. *See* Press Release by European Commission (Apr. 25, 2023, Brussels) *Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines*, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413; *see also* Press Release by European Commission (Dec. 20, 2023) *Commission Designates Second Set of Very Large Online Platforms under the Digital Services Act*, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6763.

[28] TCO Regulation, *supra* note 17.

[29] *See* the extensive definition of "terrorist content" in the TCO Regulation, *supra* note 17, art. 2 (7).

[30] *Id.* art. 3(3).

[31] *Id.* art. 9.

[32] *Id.* art. 10.

[33] DSA, *supra* note 5, art. 2(4)(c).

the Audiovisual Media Services Directive, which was revised in 2018 and contains new rules on how video-sharing platforms (e.g., YouTube) shall deal with illegal content.[34]

3.1.3 *Regulatory Initiatives of the Member States*

It is not only the European legislator who has contributed to making the regulatory landscape in Europe increasingly complex through sector-specific regulation. Member States have also contributed to this by introducing national legislation on digital services and online platforms. For example, as the ECD does not contain any harmonized rules on notice-and-action procedures, several Member States have enacted such rules in their national legislation.[35] In addition, some Members more recently introduced strict requirements for platforms to remove specific types of illegal content (e.g., illegal hate speech) within a short time frame. A prominent and rather controversial example is the German Network Enforcement Act (NetzDG) of 2017, which stipulates due diligence obligations for social media platforms.[36] In particular, the NetzDG specifies that content that is "manifestly unlawful" must be removed or blocked within twenty-four hours of receiving a complaint.[37] Other examples of national platform laws that require the deletion of illegal content within short time limits include the Austrian Communication Platforms Act[38] and the French Loi Avia (although key provisions of the latter were struck down by the French Constitutional Council in June 2020).[39] These national initiatives and the growing risk of regulatory fragmentation was one of the main drivers of the European Commission's effort to update the legislative framework for online

[34] AVMS Directive, *supra* note 15.

[35] *See* Impact Assessment accompanying the Proposal for a Digital Services Act, SWD (2020) 348 final, 28–29, https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-services-act.

[36] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken [Netzwerkdurchsetzungsgesetz] [NetzDG] [Act to Improve Enforcement of the Law in Social Networks] Bundesgesetzblatt, Teil I 3352 (Sept. 1, 2017), translation at https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG-engl.pdf; for a critical evaluation, *see, e.g.*, Rebecca Zipursky, *Nuts about NETZ: The Network Enforcement Act and Freedom of Expression*, 42 Fordham Int'l L.J. 1325 (2019); Patrick Zurth, *The German NetzDG as Role Model or Cautionary Tale? Implications for the Debate on Social Media Liability*, 31 Fordham Intell. Prop. Media & Ent. L.J. 1084 (2021).

[37] NetzDG, *supra* note 35, art. 3(2)(ii).

[38] Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen [Kommunikationsplattformen-Gesetz] [KoPl-G] [2020] BGBl. I Nr. 151/2020.

[39] Décision 2020-801 DC du 18 juin 2020 visant à lutter contre les contenus haineux sur internet [Law 2020-801 of June 18, 2020 aiming to counter hateful content on the internet], Journal Officiel de la République Française 0156 [J.O.] [Official Gazette of France], June 25, 2020; *see also* Aurelien Breeden, *French Court Strikes Down Most of Online Hate Speech Law*, N.Y. Times (June 18, 2020), https://www.nytimes.com/2020/06/18/world/europe/france-internet-hate-speech-regulation.html.

platforms and ensure that platforms are regulated at the EU level.[40] In November 2023, the European Court of Justice decided that national laws may not subject a communication platform provider established in another Member State to general and abstract obligations (e.g., reporting obligations).[41] In its decision, the Court held that such a regulatory approach would be in breach of the ECD's country-of-origin principle. This ruling further limits the regulatory options of Member States vis-à-vis online platforms.

3.1.4 *The Digital Services Act*

In December 2020, the European Commission published the then much-anticipated proposal[42] for a Digital Services Act (DSA) to update the regulatory framework for online platforms.[43] The proposal was part of a more comprehensive legislative package that also includes the Digital Markets Act (DMA).[44] Together, the DSA and the DMA create a new regulatory framework for the governance of digital services in the European Union.[45] The DMA aims at ensuring a contestable and fair market across the digital sector by stipulating *ex ante* rules applicable only to large online platforms that act as "gatekeepers"[46] between business users and end users.[47] In contrast, the DSA has a much broader scope and aims at updating the existing rules on platform responsibility for the provision of digital services.

[40] Buri and van Hoboken, *supra* note 14, at 6

[41] CJEU Case C-376/22, Google Ireland and Others, ECLI:EU:C:2023:835 (Nov. 9, 2023).

[42] DSA Proposal, *supra* note 3; for an overview see Christoph Busch & Vanessa Mak, *Putting the Digital Services Act in Context: Bridging the Gap between EU Consumer Law and Platform Regulation*, 10 Journal of European Consumer and Market Law 109 (2021); *see also* Miriam C. Buiten, *The Digital Services Act: From Intermediary Liability to Platform Regulation*, 12 J. JIPITEC 361 (2021).

[43] This section draws on Christoph Busch, *Regulating the Expanding Content Moderation Universe: A European Perspective on Infrastructure Moderation*, 27 UCLA Journal of Law & Technology 32 (2022).

[44] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), http://data.europe.eu/eli/reg/2022/1925/oj (hereinafter *DMA*).

[45] *See* Martin Eifert, Axel Metzger, Heike Schweitzer & Gerhard Wagner, *Taming the Giants, The DMA/DSA Package*, 58 Common Market Law Review 987 (2021).

[46] On September 6, 2023, The European Commission has designated Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft as "gatekeepers" under the Digital Markets Act, requiring them to comply with its regulations within six months for their twenty-two core platform services. *See* Press Release by European Commission (Sept. 6, 2023, Brussels) *Digital Markets Act: Commission Designates Six Gatekeepers*, https://perma.cc/KR8U-JQ8D.

[47] *See* Alexandre de Streel, *The European Proposal for a Digital Markets Act – A First Assessment* (Jan. 19, 2021), https://cerre.eu/publications/the-european-proposal-for-a-digital-markets-act-a-first-assessment.

3.1.4.1 General Framework of Platform Liability

Regarding platform liability, the DSA keeps up the conditional exemptions from liability of providers of online services.[48] One important difference compared to the ECD is that they will be contained in an EU Regulation, which unlike EU Directives requires no implementing legislation within individual Member States and therefore increases the level of harmonization.[49] Generally speaking, the DSA makes three contributions to the regulatory framework for content moderation by (1) setting out general rules of liability for providers of intermediary services; (2) establishing a regime of due diligence obligations, with a special focus on online platforms including social media; and (3) strengthening the cooperation between national authorities in charge of the public enforcement of online regulation.[50]

The liability rules for providers of online intermediary services set out in Chapter II of the DSA form the legal backdrop for content-related decisions taken by platform operators and other providers of digital intermediary services.[51] These rules determine under which circumstances online intermediaries, such as ISPs, hosting providers, or social media platforms, are legally required to remove content. The DSA abstains from the difficult task of drawing a line between legal and illegal content. Instead, it defines a number of liability exemptions by establishing when a provider of online intermediary services *cannot* be held liable in relation to third-party content. The safe harbor regime of the DSA broadly follows the existing model of the ECD.[52]

The DSA defines liability exemptions based on an intermediary's specific functions: mere conduit,[53] caching,[54] and hosting.[55] For the first two categories of providers, the DSA establishes a broad liability exemption as long the providers are "in no way involved with the information transmitted."[56] In contrast, for hosting providers, legal immunity is based on a knowledge standard. In other words, the DSA shields hosting providers from liability only if they do not know that they are hosting illegal content. This general rule is supplemented by two important limitations: First, Member states must not impose a general obligation to monitor content

[48] For an overview, *see* Martin Husovec, Principles of the Digital Services Act (forthcoming).
[49] *See* art. 288 of the Treaty on the Functioning of the European Union (TFEU).
[50] *See*, *e.g.*, Martin Eifert et al., *supra* note 43.
[51] *See* DSA, *supra* note 5, arts. 4–10.
[52] *See* ECD, *supra* note 1, arts. 12–13; *see also* Sebastian Felix Schwemer et al., *Liability Exemptions of Non-Hosting Intermediaries: Sideshow in the Digital Services Act?*, 8 Oslo L. Rev. 4, 27 (2021) (discussing the liability exemptions for non-hosting providers under the ECD).
[53] DSA, *supra* note 5, art. 4.
[54] *Id.* art. 5.
[55] *Id.* art. 6.
[56] *Id.* recital 21.

on providers.[57] Second, it incorporates a Good Samaritan rule, whereby providers who carry out self-initiated investigations in order to detect and remove illegal content will not lose their liability exemption for this reason alone.[58]

3.1.4.2 Due Diligence Obligations

The above liability rules are complemented by several due diligence obligations for online intermediaries. Because of the broad range of intermediary services covered by the new rules, the DSA does not apply a one-size-fits-all approach. Instead, it follows a "risk-based approach" and formulates a catalog of "asymmetric due diligence obligations."[59] In doing so, the DSA distinguishes four levels of regulation:

Level 1 contains a basic set of rules, which applies to the broadest category, that is, all providers of online intermediary services. This category includes all providers of mere conduit, caching and hosting services.[60]

Level 2 applies to all providers of hosting services, such as cloud storage providers and webhosting services.[61]

Level 3 contains some additional provisions that apply only to online platforms,[62] defined as a provider of hosting services that, at the request of a recipient of the service, stores and disseminates to the public information.[63] This category includes online marketplaces, social networks, and app stores.

Level 4 adds some specific due diligence obligations for "very large online platforms" (VLOPs), and "very large online search engines" (VLOSEs), which have more than forty-five million average monthly EU users (i.e., roughly 10 percent of EU citizens).[64] In contrast, very small platforms are exempt from most due diligence obligations.[65]

This model of asymmetric regulation, under which the rules become more numerous and stricter as we go from Level 1 to Level 4, is an expression of the principle of proportionality. In terms of substance, the DSA introduces, for the first time, a number of due diligence obligations with regard to content moderation. For example, all providers of online intermediary services have to include information about their content moderation policy in their terms and conditions.[66] They also

[57] *Id.* art. 8.
[58] *Id.* art. 7.
[59] DSA Proposal, *supra* note 3, at 6.
[60] *See* DSA, *supra* note 5, arts. 11–15.
[61] *Id.* arts. 16–18.
[62] *Id.* arts. 19–32.
[63] *Id.* art. 3(i).
[64] *Id.* arts. 33–43.
[65] *See, e.g., id.* arts. 19, 29.
[66] *Id.* art. 14(1).

have to publish annual reports with meaningful and comprehensive information about their content moderation activities, including details on the use of automated tools for content moderation (*Level 1*).[67] In addition to these general requirements, providers of hosting services must provide harmonized notice-and-action mechanisms and justify removal decisions with a statement of reasons (*Level 2*).[68] Providers of online platforms must also provide users with meaningful possibilities to challenge decisions to remove or label content via an internal complaint system and an external out-of-court dispute resolution mechanism (*Level 3*).[69] Finally, VLOPs and VLOSEs are subject to additional rules to ensure more comprehensive public oversight of their content moderation practices (*Level 4*). In particular, VLOPs and VLOSEs are obliged to develop appropriate tools for assessing and managing systemic risks and take measures to protect the integrity of their services against manipulation, including disinformation campaigns or interference with electoral processes.[70]

Most of the rules regarding content moderation in the DSA have been drafted with user-facing platforms such as Facebook, Twitter, or YouTube in mind. But the DSA also responds to the expansion of content moderation practices by expanding its content moderation rules, both in the horizontal and vertical dimensions.[71] In this sense, some of the content moderation rules stipulated by the DSA apply also to nontraditional platforms (e.g., public groups on messaging services) and to actors deeper down in the content moderation stack (e.g., cloud services, content delivery networks).

3.2 ENFORCEMENT OF PLATFORM RESPONSIBILITY RULES

Enforcement of platform responsibility was a weak spot of the ECD, which mainly relied on self-regulatory initiatives and gave Member States wide discretion regarding the choice of enforcement methods (Section 1).[72] In contrast, the DSA puts a strong emphasis on procedural aspects and enforcement.[73] In doing so, it combines different methods including self-regulation and administrative liability (Section 2).

[67] *Id.* art. 16.
[68] *Id.* arts. 16–17.
[69] *Id.* arts. 20–24.
[70] *Id.* arts. 33–43.
[71] *See* Busch, *supra* note 40.
[72] *See, e.g.*, Melanie Smith, *Enforcement and cooperation between Member States: E-Commerce and the future Digital Services Act, Study for the IMCO committee of the European Parliament* (Apr. 2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648780/IPOL_STU(2020)648780_EN.pdf.
[73] *See, e.g.*, Ilaria Buri & Joris van Hoboken, *The DSA Supervision and Enforcement Architecture* (DSA Observatory, June 24, 2022), https://dsa-observatory.eu/2022/06/24/the-dsa-supervision-and-enforcement-architecture/.

3.2.1 *The E-Commerce Directive: Self-regulation and Wide Discretion for Member States*

The ECD did not provide for an effective oversight and enforcement framework at the European level. Instead, it merely suggested that the European Commission and Member States encourage the drawing up of codes of conduct by trade, professional, and consumer organizations.[74] Examples of such codes are the above-mentioned EU Code of Practice on Disinformation,[75] the EU Code of conduct on countering illegal hate speech online,[76] and the EU Product safety pledge.[77] With regard to civil liability and private rights to sue, the ECD only vaguely instructs Member States to "ensure that court actions available under national law allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and prevent any further impartment of the interests involved."[78] Regarding administrative enforcement, the ECD mainly limits itself to stipulating that "Member States shall have adequate means of supervision and investigation necessary to implement" the ECD.[79] Similarly, the ECD does not prescribe which type of sanctions Member States shall apply to infringements of national provisions implementing the ECD. Instead, the choice of sanctions is left to the discretion of Member States. Using the standard formula of EU Directives, the ECD merely stipulates that those sanctions shall be "effective, proportionate and dissuasive."[80]

3.2.2 *The Digital Services Act: Strong Emphasis on Oversight, Enforcement, and Sanctions*

Unlike the ECD, the DSA puts a strong emphasis on oversight and enforcement and devotes a detailed chapter on "implementation, cooperation, sanctions and enforcement."[81] Generally speaking, the enforcement of the due diligence obligations imposed by the DSA on platforms is shared between Member States and the European Commission. For starters, the Member State where the platform has its

[74] ECD, *supra* note 1, art. 16(1)(a).
[75] *See supra*, note 18.
[76] *See supra*, note 16.
[77] *See* European Commission, Product Safety Pledge: Voluntary commitment of online marketplaces with respect to the safety of non-food consumer products sold online by third party sellers (June 25, 2018), https://ec.europa.eu/info/sites/default/files/voluntary_commitment_document_2021_v5.pdf; *see also* European Commission, 6th Progress Report on the implementation of the Product Safety Pledge (Apr. 22, 2022), https://ec.europa.eu/info/sites/default/files/6th_progress_report_product_safety_pledge.pdf.
[78] ECD, *supra* note 1, art. 18(1)(a).
[79] *Id.* art. 19(1).
[80] *Id.* art. 20.
[81] DSA, *supra* note 5, Chapter IV, arts. 49–88.

main establishment will have exclusive powers for the supervision of the DSA rules, except where such powers are attributed to the exclusive or shared competence of the European Commission.[82] In particular, the European Commission is granted exclusive powers regarding the specific obligations set out in Section 4 Chapter III DSA, which apply only to large online platforms (VLOPs) and very large online search engines (VLOSEs). For fulfilling this role, the Commission is granted far-reaching powers of investigation, enforcement, and monitoring (similar to those in antitrust cases) in respect of VLOPs and VLOSEs.[83] In December 2023, the European Commission has opened formal proceedings against the social media platform X (formerly Twitter) in order to investigate whether X may have breached its obligations under the DSA regarding risk management, content moderation, dark patterns, advertising transparency, and data access for researchers.[84]

For coordinating the enforcement of the DSA, each Member State must appoint a Digital Services Coordinator (DSC).[85] The DSC will be an independent authority responsible for supervising platforms and other intermediary services in their Member State and for coordinating supervision by sectoral authorities. It is envisaged that national DSCs and the Commission cooperate closely and provide each other mutual assistance in the enforcement of the DSA. Cooperation between DSCs shall be facilitated by the setting up of a European Board for Digital Services, which consists of all national DSCs and the European Commission.[86]

The DSA is also more explicit with regard to the type of sanctions that may be imposed in case of infringements. In particular, the DSA states that the competent enforcer – the DSC or the European Commission, as the case may be – can, in the most serious cases, impose a fine of up to 6 percent of the total worldwide annual turnover in the preceding financial year.[87] Moreover, periodic penalty payments of up to 5 percent of the average daily income or worldwide annual turnover in the preceding financial year per day may be imposed.[88]

As this brief overview shows, the DSA focuses on public enforcement and introduces a centralized regulatory model for VLOPs and VLOSEs with the Commission as the primary regulator. The choice of this model seems to be

[82] *Id.* art. 56(1). For platforms which do not have an establishment in the EU, the Member State where the legal representative (as required under art. 13 DSA) is established or the European Commission (in case of VLOPs and VLOSEs) shall have powers for the supervision (arts. 56(2), 56(6) DSA). If a platform fails to appoint a legal representative, all Member States or the European Commission (in case of VLOPs and VLOSEs) have those powers (art. 56(7) DSA).

[83] DSA, *supra* note 5, arts. 64–83 (including, for example, the power to request information, take interviews and conduct inspections).

[84] *See* Press Release by European Commission, Commission opens formal proceedings against X under the Digital Services Act (Dec. 18, 2023), https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6709.

[85] *Id.* art. 49.

[86] *Id.* art. 61.

[87] *Id.* arts. 52(3) and 74(1).

[88] *Id.* arts. 52(4) and 76.

influenced by the difficulties that have arisen in enforcing the General Data Protection Regulation[89] (GDPR).[90] In particular, it occurred that some national data protection authorities were rather slow to respond to complaints and requests for cross-border cooperation by authorities from other Member States. Against this background, the DSA also establishes a detailed cooperation mechanism that seeks to ensure that the enforcement of the DSA will not be compromised by an inactive DSC. In particular, in case of disagreement among DSCs, the European Board for Digital Services may refer the matter to the Commission in order to speed up the enforcement procedure.[91]

While the DSA focuses on administrative enforcement, it is important to note that the public enforcement model is complemented also by other methods of enforcement. In this sense, Art. 54 DSA, which was introduced only during the trilogue negotiations between the European Commission, the European Parliament, and the Council of the European Union, underlines that platform users "shall have the right to seek, in accordance with Union and national law, compensation from providers of intermediary services, against any damage or loss suffered due to an infringement by those providers of their obligations" under the DSA. In other words, a violation of the due diligence obligations stipulated by the DSA may also give rise to civil liability. However, the DSA leaves the details of such individual claims to the laws of the Member States. Finally, violations of the DSA may also give rise to class actions (or, more precisely, "representative actions") under Directive (EU) 2020/1828.[92]

3.3 SPECIFIC PLATFORM RESPONSIBILITIES REGARDING CONTENT MODERATION

Content moderation by digital platforms has become a focal point of the policy debate on platform regulation.[93] Some argue that platforms are not doing enough to reduce the dissemination of illegal or harmful content. Others criticize platforms for exercising too much censorship. Against this background, this section will explain how the DSA regulates content moderation by platforms, in particular the scope of

[89] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) (hereinafter *GDPR*).

[90] *See* Buri and van Hoboken, *supra* note 14; *see also* Buiten, *supra* note 39, para. 78.

[91] *See* DSA, *supra* note 5, art. 59.

[92] *Id.* art. 90.

[93] *See generally* James Grimmelmann, *The Virtues of Moderation*, 17 YALE J. L. & TECH 42 (2015); Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149 (2018); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018); Hannah Bloch-Wehba, *Automation in Moderation*, 53 CORNELL INT'L L. J. 41 (2020).

platform responsibility for detection and moderation, and limits on platform discretion to moderate.

3.3.1 *General Framework: No General Monitoring Obligations and Good Samaritan Rule*

The DSA defines content moderation as "activities, automated or not, undertaken by providers of intermediary services that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service."[94] As mentioned before, such activities to detect and moderate specific types of content are not only taken by operators at the platform level but also deeper down in the internet stack at the infrastructure level.[95] The definition provided by the DSA is rather broad in two respects: first, it not only covers decisions to remove content and disable user accounts but also other measures that influence the "availability, visibility and accessibility" of content, such as downranking and de-amplification. Second, the definition is not limited to "illegal content" but also includes measures taken with regard to information which is incompatible with the terms and conditions of the online service provider. Therefore, content moderation under the DSA includes also measures taken regarding content that is legal but nevertheless considered objectionable.

As explained in Section 3.1, the DSA establishes a knowledge-based limited liability regime that is built around a notice-and-action mechanism. These rules determine under which circumstances online intermediaries, including social media platforms, are legally required to remove content. In this sense, the liability rules for providers of online intermediary services form the legal backdrop for content-related decisions taken by online platforms.[96] Another key provision that determines the legal framework for content moderation decisions is Art. 8 DSA, which underlines that "no general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers." While any "general obligation" to monitor is prohibited, courts may impose "specific obligations" to monitor activities on the platform in order to tackle repeat infringers or the reappearance of identical or content with "equivalent meaning."[97]

[94] *See* DSA, *supra* note 5, art. 3(t). According to this definition moderation activities may include "measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetization, disabling of access to, or removal thereof, or that affect the ability of the recipients to provide that information, such as the termination or suspension of a recipient's account."

[95] *See* Busch, *supra* note 40.

[96] *See* DSA, *supra* note 5, arts. 4–10.

[97] *See, e.g.*, CJEU Case C-18/18, Glawischnig-Piesczek v. Facebook, ECLI:EU:C:2019:821 (Oct. 3, 2019).

A notable addition to the EU regime of platform liability is Art. 7 DSA, on "voluntary own-initiative investigations." According to Art. 7 DSA, online intermediaries will not automatically lose the conditional exemption from liability "solely because" they carry out voluntary investigations or take other measures for "detecting, identifying and removing, or disabling access to, illegal content" or "take the necessary measures to comply with" requirements of national law or EU law, including those set out in the DSA. The purpose of Art. 7 DSA is to incentivize online intermediaries to engage in voluntary content moderation of harmful and illegal content by introducing a sort of "Good Samaritan" protection.[98] It is unclear, however, whether this aim will be achieved. In particular, the scope of the protection offered by Art. 7 DSA will need further clarification. During the trialogue negotiations between the European Commission, the European Parliament, and the Council of the European Union, the wording of the provision has been amended to the effect that voluntary own-initiative investigations are only covered by the Good Samaritan protection if they are carried out "in good faith and in a diligent manner". It is unclear, however, which level of diligence is required with regard to content moderation activities by platforms. At least some clarification is provided by Recital 26 of the DSA, which underlines that the condition of acting in good faith and in a diligent manner should include "acting in an objective, non-discriminatory and proportionate manner and with due regard to the rights and legitimate interests of all parties involved." While the DSA does not formulate an explicit requirement of platform neutrality, the reference to the principle of non-discrimination makes it clear that an arbitrary unequal treatment of content within the framework of content moderation would be a violation of the due diligence requirements.

3.3.2 *Asymmetric Due Diligence Obligations: Risk-Based Approach to Content Moderation*

In addition to the general rules set out in Arts. 7–8 DSA, there are a number of more specific rules on content moderation that are scattered throughout the DSA. These rules stipulate graduated due diligence obligations regarding content moderation depending on the type and size of intermediary. In this sense, they follow the asymmetric model ("risk-based approach") of the DSA.

3.3.2.1 Transparency and Reporting

According to Art. 14(1) DSA all providers of intermediary services, including social media platforms, must provide in their terms and conditions "information on any restrictions that they impose in relation to the use of their service." This information

[98] *See* Buri and van Hoboken, *supra* note 14, at 17.

shall include details on "any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making, and human review as well as rules of procedure of their internal complaint handling system."

These general transparency requirements are supplemented by Art. 15 DSA, which stipulates detailed reporting obligations.[99] In particular, it requires providers of intermediary services to publish a yearly report on any content management they engaged in during the relevant time period.[100] This report shall provide "meaningful and comprehensible information about the content moderation engaged in at the providers' own initiative."[101] Furthermore, detailed information about the use of "automated means for the purpose of content moderation" must be included in the report.[102]

On September 26, 2023, the European Commission launched the DSA Transparency Database, a first-of-its-kind platform that collects data in accordance with Art 25(5) of DSA and provides public access to content moderation decisions made by online platform providers in the EU. This initiative aims to enhance online transparency and accountability.[103]

3.3.2.2 Fundamental Rights and Proportionality

The DSA not only stipulates transparency and reporting requirements regarding content moderation policies but also regulates how providers of intermediary services shall implement their content moderation procedures. Pursuant to Art. 14(4) DSA, they "shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions" referred to Art. 14(1), "with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter."[104] In other words, Article 14(4) DSA sets a benchmark for content moderation decisions by providers at all levels of the content moderation stack. All providers of intermediary services are obliged to take due consideration of

[99] Providers of intermediary services that qualify as "micro or small enterprises" within the meaning of Recommendation 2003/361/EC are exempt from the reporting obligations. DSA, *supra* note 5, art. 13(2).

[100] DSA, *supra* note 5, art. 13(1).

[101] *Id.* art. 15(1)(c). This information shall include details about the "use of automated tools, the measures taken to provide training and assistance to persons in charge of content moderation."

[102] *Id.* art. 15(1)(e). In this regard, the reports shall include "qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied."

[103] Press Release by European Commission (Sept. 26, 2023) *Digital Services Act: Commission launches Transparency Database*, https://digital-strategy.ec.europa.eu/en/news/digital-services-act-commission-launches-transparency-database.

[104] *Id.* art. 14(4).

fundamental rights enshrined in the EU Charter of Fundamental Rights (CFR),[105] particularly the freedom of expression and information, the freedom to conduct a business, and the right to nondiscrimination.[106]

Similarly, Recital 47 of the DSA underlines that the design, application, and enforcement of content-related restrictions should be "non-arbitrary and non-discriminatory." It remains to be seen whether these references to the principle of nondiscrimination will be interpreted by the European Court of Justice as the legal foundation of a requirement of neutrality with regard to content moderation. In this context, it might also be of interest that during the legislative process, a possible prohibition of content moderation for media content was discussed.[107] On the one hand, it was argued that such a prohibition could strengthen the independence of the media, but, on the other hand ,it could undermine the goal of tackling disinformation. Finally, the proposed ban was not included in the text of the provisional agreement on the DSA.

3.3.2.3 Notice-and-Action Mechanism and Complaint Handling

The DSA requires providers of hosting services, including providers of online platforms, to set up a user-friendly electronic *notice-and-action mechanism* that allows "any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content."[108] This mechanism shall enable users to notify hosting service providers of allegedly illegal content. If such a notice is sufficiently substantiated and fulfills the requirements set out in Art. 16(2) DSA, the provider is considered to have actual knowledge of the illegal activity. This triggers application of the liability rule under Art. 6 DSA. In other words, the hosting service provider will be liable for the illegal content unless the provider "acts expeditiously to remove or to disable access to the illegal content."[109] However, providers are only deemed to have actual knowledge of the illegal content where the notices "allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without detailed legal examination."[110] If a hosting provider decides to remove or disable access to the illegal content or otherwise restricts the visibility of specific items of information,

[105] *See* Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) [hereinafter *CFR*].
[106] DSA, *supra* note 5, art. 14(4). *See also*, *id.*, recital 3; CFR, arts. 11, 16, 21.
[107] *See* Julian Jaursch, *No Content Moderation for Media Publishers? Proposed Amendment for Digital Services Act Is a Lesson in Unintended Consequences*, Tech Policy Press (Nov. 10, 2021), https://techpolicy.press/no-content-moderation-for-media-publishers-proposed-amendment-for-digital-services-act-is-a-lesson-in-unintended-consequences/.
[108] DSA, *supra* note 5, art. 16(1).
[109] *Id.* art. 6(1)(b).
[110] *Id.* art. 16(3).

Art. 17 DSA obligates the host to provide the uploader of that content with a detailed statement of reasons for removal.[111]

For online platforms, the DSA adds a further element to increase the effectiveness of the notice-and-action mechanism. Pursuant to Art. 22(1) DSA, providers of online platforms shall take the necessary technical and organizational steps to cooperate with specialized "trusted flaggers" (e.g., consumer organizations or other NGOs) and to ensure that notices provided by them are decided upon with priority.[112] Providers of online platforms are also obliged to set up an internal *complaint-handling system*, which enables users to lodge a complaint against decisions to remove content or terminate the service.[113] Furthermore, users who are affected by the provider's decision must be given the opportunity to appeal the decision to an impartial dispute resolution body whose decision is binding on the platform provider.[114]

3.3.2.4 Systemic Risk Management

For very large online platforms (VLOPs) and very large online search engines (VLOSEs), the DSA provides even more extensive regulations.[115] They will be required to undergo annual risk assessments to identify any significant systemic risks stemming from the services.[116] The scope of this risk assessment includes the "dissemination of illegal content," "any actual or foreseeable negative effects for the exercise of fundamental rights," and "any actual or foreseeable negative effects on civic discourse and electoral processes, and public security."[117] When assessing such systemic risks, several factors shall be taken into account, including the design of recommender systems and "other relevant algorithmic systems"[118] as well as the functioning of the content moderation systems.[119]

In order to counter the above-mentioned systemic risks, VLOPs and VLOSEs must put in place reasonable, proportionate, and effective mitigation measures. Such measures may include adapting their content moderation systems (e.g., by adjusting the speed and quality of processing notices related to specific types of illegal content) or by adjusting their terms and conditions.[120] The effectiveness of

[111] *Id.* art. 17(1).
[112] The status of "trusted flaggers" is awarded by the national Digital Services Coordinators. DSA, *supra* note 5, art. 22(2).
[113] *Id.* art. 20.
[114] *Id.* art. 21.
[115] *Id.* arts. 33–43.
[116] *Id.* art. 34.
[117] *Id.*
[118] *Id.* art. 34(2)(a).
[119] *Id.* art. 34(2)(b).
[120] DSA, *supra* note 5, art. 35.

these measures will be assessed at least annually by an independent audit.[121] Furthermore, VLOPs and VLOSEs are required to publish transparency reports every six months, as opposed to once a year.[122]

Influenced by the conflict in Ukraine, a new "crisis response mechanism" was introduced into the final version of the DSA during the trialogue negotiations,[123] which sparked a controversial debate.[124] Under this provision, the European Commission may require VLOPs to react to a public security or public health crisis by initiating an urgent crisis response. For example, VLOPs could be required to intensify their fight against the dissemination of disinformation. Such measures may include, for example, "adapting content moderation processes and increasing the resources dedicated to content moderation."[125] Similarly, VLOPs may be obliged to take "awareness-raising measures" and promote "trusted information."[126]

3.4 INTERNATIONAL ASPECTS OF PLATFORM RESPONSIBILITY

This final section will briefly address three aspects that may be of particular relevance for US readers: the application of EU platform responsibility rules to platform operators based outside the EU (Section 1), the obligation to designate a legal representative in the EU (Section 2), and the global reach of court orders to remove certain content (Section 3).

3.4.1 *Application to Foreign-Based Platforms*

The DSA will have extraterritorial reach beyond the EU. More precisely, the rules set out in the DSA will apply to all intermediary service providers, irrespective of their place of establishment, to the extent that they provide services to users in the EU.[127] Whether the intermediary services are provided in the EU is determined by a "substantial connection" test. A substantial connection is deemed to exist where the provider either has an establishment in the European Union or, its absence, on the basis of the existence of a significant number of users in the EU or the targeting of activities toward one or more EU Member States.[128] This regulatory approach

[121] *Id.* art. 37.
[122] *Id.* art. 42. In particular, the report must provide details about the results of the risk assessment (art. 34), the risk mitigation measures (art. 35), and the independent audit (art. 37).
[123] DSA, *supra* note 5, art. 36.
[124] *See* Morgan Meaker, *Ukraine War Prompts Europe's New Emergency Rules for the Internet*, WIRED (Apr. 25, 2022), https://www.wired.com/story/europe-digital-services-act/.
[125] DSA, *supra* note 5, Recital 91.
[126] *Id.*
[127] *Id.* art. 2(1).
[128] *Id.* Recital 8 ("The targeting of activities towards a Member State could also be derived from the availability of an application in the relevant national application store, from the provision of local advertising or advertising in the language used in that Member State, or from the

follows the model of other EU instruments such as the GDPR[129] and the Regulation on addressing the dissemination of terrorist content.[130]

3.4.2 *Requirement to Designate a Legal Representative in the EU*

The extraterritorial application of the DSA would fail in practice if the competent authorities were unable to enforce the rules against a platform operator that does not have an establishment in the EU. Therefore, the DSA requires service providers based outside the EU to designate a legal representative in one of the EU Member States.[131] The representatives shall not merely be a "mailbox" for communications by Member States' authorities, but they can be held liable for noncompliance with the obligations under the DSA.[132] Similar obligations to designate a "representative" or a "responsible person" have been stipulated in other EU laws with an extraterritorial reach, such as the General Data Protection Regulation,[133] the Market Surveillance Regulation,[134] and the recent proposal for a General Product Safety Regulation.[135] Also the Regulation on addressing the dissemination of terrorist content online requires platforms that do not have their main establishment in the EU are required to designate a legal representative in the EU "for the purpose of the receipt of, compliance with and the enforcement of removal orders and decisions issued by the competent authorities."[136]

3.4.3 *Global Reach of Court Orders to Remove Content*

Another issue that may be of interest from a US perspective is the territorial scope of court orders to remove content. In this context, the recent decision of Court of Justice of the European Union (CJEU) in *Glawischnig-Pieczik v. Facebook* gave rise

handling of customer relations such as by providing customer service in the language generally used in that Member State.").

[129] *See* GDPR, *supra* note 85, art. 3.

[130] *See* TCO Regulation, *supra* note 17, art. 1(2).

[131] DSA, *supra* note 5, art. 13(1).

[132] *Id.* art. 13(3).

[133] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119), 48–49.

[134] Regulation 2019/1020, of the European Parliament and of the Council of 20 June 2019 on Market Surveillance and Compliance of Products and Amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, 2016 O.J. (L 169), 14.

[135] European Commission, Proposal for a Regulation of the European Parliament and of the Council on General Product Safety, Amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and Repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, at 42, COM (2021) 346 final (June 30, 2021).

[136] *See* TCO Regulation, *supra* note 17, art. 17(1).

to concern.[137] In the case, which concerned a defamatory post on Facebook, the Austrian Supreme Court issued a preliminary ruling request to the CJEU. Among other things, the CJEU was asked whether a national court could extend an injunction against Facebook so that it had effect worldwide. The CJEU dealt with this question rather briefly and underlined that the ECD does not impose any territorial limitation on the scope of the measures that Member States are entitled to adopt. Therefore, the CJEU argued that the ECD "does not preclude those injunction measures from producing effects worldwide."[138] However, as the Court underlined, it is necessary to take due account of the relevant international law.[139] Unfortunately, the CJEU did not further elaborate on how a worldwide effect could be reconciled with public and private international law. This was a missed opportunity considering that only a few days earlier, in *Google France v. CNIL*, the CJEU had decided that a de-referencing request based on the "right to be forgotten" under Art. 17 GDPR does not oblige a search engine to carry out a worldwide de-referencing.[140]

[137] Glawischnig-Piesczek v. Facebook, *supra* note 93.
[138] *Id.* para. 50
[139] *Id.* para. 51, 53.
[140] CJEU Case C-507/17, Google France v. CNIL, ECLI:EU:C:2019:772 (Sept. 24, 2019).