The Digital Services Act: Online Risks, Transparency and Data Access

Marie-Therese Sekwenz & Rita Gsenger

Abstract

The Digital Services Act (DSA) represents a landmark legislative framework in the European Union, aimed at regulating online platforms, enhancing transparency, and mitigating systemic risks associated with digital services. The Act aligns with broader EU regulatory efforts, including the General Data Protection Regulation (GDPR) and the Artificial Intelligence (AI) Act, positioning it as a cornerstone of digital governance.

A key objective is to create a harmonized internal market that prevents regulatory fragmentation while ensuring consumer protection and fundamental rights. The DSA introduces obligations for intermediary services, including very large online platforms (VLOPs) and very large online search engines (VLOSEs). Moreover, the regulation mandates due diligence measures such as transparency reporting, algorithmic accountability, and user rights protections. Transparency mechanisms include the publication of terms and conditions databases, the Statement of Reasons repository, and advertising libraries. Moreover, the DSA enforces structured risk assessment and mitigation strategies, particularly for systemic risks such as illegal content dissemination, disinformation, and fundamental rights violations.

A core component of the DSA is its approach to content moderation, introducing user empowerment mechanisms such as Trusted Flaggers, internal complaint-handling systems, and out-of-court dispute resolution bodies. Additionally, the Regulation includes crisis response provisions enabling swift intervention by the European Commission in extraordinary circumstances. To ensure compliance, the DSA establishes independent audit requirements and risk-based oversight mechanisms, reinforcing platform accountability. This Chapter aims to give an overview and comprehensive introduction to these provisions.

1. Introducing the DSA: Context and scope

The most important European legislative act currently regulating (large) online platforms and their content moderation systems is the Digital Services Act (DSA). The DSA is the legal update of the E-Commerce Directive (2000/31/EC) of 2000 and expands the original scope by going beyond the regulation only of individual rights (Kaesling, 2023, p. 552). The wording of the Directive did not take into account the importance that social networks and online marketplaces would play in daily life as the digital economy has developed into a platform economy (Rodríguez de las Heras Ballel, 2021, p. 80); furthermore, the scale of the services and the multiplication of various intermediaries needed to be considered. Differing legislative efforts of Member States led to the fragmentation of legal regulations and challenges regarding the enforcement of services that operate across borders (Schwemer, 2023, p. 233). Moreover, the important role of algorithmic decision-making (Castellucia and Le Métayer, 2019; Dogru. Facciorusso and Stark, 2020), disinformation (Bayer et al, 2021; Iosifidis and Nicoli, 2021), and illegal content (De Streel et al, 2020; Kübler et al, 2021) has become more evident.

The general aim of the DSA is a "safe, predictable and trusted online environment" (Art. 1 (1) DSA) through the realisation of an internal European market. Since platforms operate transnationally and Member States may have their own rules, there is a risk that the market might fragment, as occurred with the regulatory attempts of Germany (Network Enforcement Act, 2017) and Austria (Communication Platforms Act, 2020). An internal market would enable companies to benefit from unification and allow them to innovate in a harmonised environment. Moreover, new markets can be accessed and consumers overall would have more choices (Hofmann and Raue, 2023, p. 33).

In December 2020, the DSA was presented in conjunction with the Digital Markets Act (DMA) (Directive (EU) 2019/790), which aims to ensure a fair platform economy with a functioning internal market (Morais Carvalho et al, 2021, p. 74). In the first Chapter, the DSA determines its subject matter (Art. 1) and scope (Art. 2) and provides definitions (Art. 3). Chapter II focuses on the liability of providers and intermediary services, and Chapter III on due diligence and transparency. Chapter III consists of sections listing the specifications concerning the obligations of different intermediary services, such as online platforms or very large online platforms (VLOPs) and search engines (VLOSEs) (as defined by Art. 33(1) DSA).

Chapter IV specifies implementation, cooperation, penalties and enforcement and includes specificities about Digital Service Coordinators (DSCs) and other relevant authorities and competencies, such as the European Board for Digital Services. The Board acts as an independent advisory body for the DSCs (Arts. 61–64 DSA); DSCs are the regulatory body situated in each Member State. Member States choose these "competent authorities" (Art. 49, (2)), and the DSCs are subsequently "responsible for all matters relating to supervision and enforcement" of the DSA in the respective Member State (Art. 49 (2)).

The DSA defines its scope in Art. 2 (1), including intermediary services (Art. 3 (g) DSA), hosting services (Art. 3 (g) (iii) DSA), online platforms (Art. 3 (i) DSA), VLOPs (Art. 33(1) DSA) and VLOSEs (Art. 3 (j) DSA) that offer their services inside the European Union.

Intermediary services refers to three types of "information society services" (lit. g): first, services that are "mere conduit" (i), transmitting information by a recipient of the service. Second, "a 'caching' service" (ii) that includes the transmission and storage of information and third, "a 'hosting' service, consisting of the storage of information provided by, and the request of, a recipient of the service" (iii). An online platform is a hosting service that, "at the request of a recipient of the service, stores and disseminates information to the public" (Art. 3 lit. i). Online search engines are also intermediary services that "allow[s] users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found" (lit. j).

VLOPs and VLOSEs are defined as services and intermediaries operating in the European Union that are reported to have more than 45 million monthly active users (Art. 33 (1)). The number of users should cover at least 10% of the EU population. The number is reported by the platforms themselves, and they must provide an updated number of monthly active users "at least once every six months" (Art. 24 (2)) or "without undue delay" (Art. 24 (3)) upon receiving a request from the European Commission. The European Commission first designated platforms and search engines considered to be very large in April 2023; now, that list is frequently updated and includes platforms such as AliExpress, Google Search, Facebook, TikTok, Meta and Amazon (European Commission, 2024a). This limit cannot be bypassed by European nation-states and no platforms with fewer

monthly active users can be obliged to adhere to the risk identification and mitigation requirements (Kaesling, 2023, p. 533). The European Commission assumes that intermediaries of this size have significant influence on the internal market and that they have sufficient resources to adhere to the Regulation (Kaesling, 2023, p. 541).

The DSA includes natural or legal persons who have the possibility of using a service (Art. 3 lit. b); such a person is referred to as a "recipient" (Art. 3 lit. b). However, the DSA also refers to persons as "users" throughout the text, and this term is preferred in this chapter as it is more commonly used. The DSA presents a legal definition that describes active users or recipients. This definition, however, is in the main text of the DSA, not in the Recitals, emphasizing the importance of the differentiation. An active user of an online platform can be classified in two ways: they can "request [...] the online platform [...] host information" (Art. 3 lit. p), meaning, for instance, uploading user-generated content to platforms or commenting on other content (Kaesling, 2023, p. 542); or, an active recipient is a person "exposed to information hosted by the online platform and disseminated through its online interface" (Art. 3 lit. p). Therefore, receiving or consuming content on platforms without contributing or uploading content is sufficient to be considered an active user. Participation is confirmed independent of registration and includes the consumption of any content (whether visual or audio) that starts without any user involvement as soon as a website opens (Kaesling, 2023, p. 542). An active recipient of a search engine "has submitted a query to an online search engine and been exposed to information indexed and presented on its online interface" (Art. 3 lit. q DSA). A query includes the input of terms, and if the query is completed automatically and the recipient presses enter, the input counts as active use (Kaesling, 2023, p. 542).

Intermediaries profit from the *Good Samaritan Clause* that limits liability and determines that they are not responsible for any content shared that might be illegal (G'sell, 2023, p. 4). Therefore, they are exempt from liability under certain conditions (Hofmann and Raue, 2023, p. 32f) and, moreover, are not required to participate in any monitoring activities (Art. 8 DSA).

Complementing the DMA[1], the DSA aims to enable citizens to exercise their fundamental rights in a safe online environment (Morais Carvalho et al, 2021, p. 75). The DSA aims to reduce risks of VLOPs and VLOSEs

1 For more information on the DMA, see Chapter 6, 'The Brave Little Tailor v. Digital Giants: A Fairy-Tale Analysis of the Social Character of the DMA' by Liza Herrmann.

by establishing clear rules and transparency. In addition to a trustworthy online environment, the DSA seeks to ensure that fundamental rights are protected and consumer protections strengthened. Lastly, the DSA aims to establish legal certainty (Hofmann and Raue, 2023, p. 33).

Similar to other European Regulations such as the General Data Protection Regulation[2], the AI Act[3] or the NIS 2 Directive[4], the DSA includes risk-based elements in its regulatory structure (Efroni, 2021). Risk detection, analysis and evaluation are thus included in the legislative package, with internal measures, external audits, transparency requirements and access reviewed by the legislature (the European Commission and DSCs) and researchers. The DSA practises "enforced self-regulation" (Kaesling, 2023, p. 532) in parts, such as systemic risk assessments (Art. 34), as the platforms are required to detect, analyse and evaluate systemic risks. That means, they – the platforms – are initially responsible; however, the compliance of platforms is tested and regularly reviewed, and in a last step, regulators intervene and enforce. The European Commission supervises the compliance of VLOPs and VLOSEs and can impose monetary sanctions (ibid.) that are not to exceed 6% of the service providers' annual turnover (Art. 52 (3). Lastly, due to Art. 88 DSA, the Commission has the ability to create Delegated Acts that detail the implementation of the DSA, for instance, on Audits (European Commission, 2023a) or the transparency reporting obligations of intermediary services (European Commission, 2023b).

In this Chapter, we will discuss the most important provisions and their consequences, including the due diligence of VLOPS and VLOSEs, including transparency mechanisms (section 2), user rights and processes (section 3), risk assessment, risk mitigation, and audits (section 4).

2. See-through regulation? Novel transparency mechanisms in the DSA

The DSA creates several new mechanisms that provide novel insights into the day-to-day decisions taken on platforms. Transparency mechanisms

2 For more information on the GDPR, see Chapter 14 'EU Data Protection Law in Action: Introducing the GDPR' by Julia Krämer.

3 For more information on the AI Act, see Chapter 2 'Searching for Harmonised Rules: Understanding the Paradigms, Provisions, and Pressing Issues in the Final EU AI Act' by Hannah Ruschemeier and Jascha Bareis, and Chapter 3 'Accountable AI: It Takes Two to Tango' by Jorge Constantino.

4 For more information on the NIS 2 Directive, see Chapter 17 'Unpacking the NIS 2 Directive: Enhancing EU Cybersecurity for the Digital Age' by Eyup Kun.

centrally include reports and databases to inform stakeholders. This text will therefore highlight the main tools of transparency by focusing on transparency reports (Art. 15, 24 and 42 DSA), the Terms and Conditions database (Art. 14 DSA), the Statement of Reasons (Art. 17 DSA) and the Ad Library, also referred to as the Ad Repository (Art. 39 DSA). Additional means of transparency can be found in the rules regarding recommendation systems (Art. 27 DSA), parameters on targeted advertising (Art. 26 DSA) and in the link between the Code of Practice of Disinformation and the DSA as a Code of Conduct (Art. 45–47 DSA) (Just and Saurwein, 2024).

Flyverbom (2016, p. 110–112) defined transparency as a complex process connected to the development, interpretation and aggregation of publishing information aimed at enhancing accountability, openness and trust within a certain period. The DSA itself does not form its own definition of transparency (Kosters and Gstrein, 2023, p. 117) but rather reflects on it in several passages, including in Recital 49: "To ensure an adequate level of transparency and accountability, providers of intermediary services should make publicly available an annual report in a machine-readable format, in accordance with the harmonised requirements contained in this Regulation". Such a machine-readable form of transparency could also enhance the automatisation of checks and balances in an empirically-based accountability regime (Murray and Flyverbom, 2020). Conversely, Kosters and Gstrein (2023) highlight the importance of the audience within the transparency regime and differentiate transparency into three layers: "The first layer of transparency involves the disclosure of information. The second layer consists of ensuring that the information disclosed is also understandable to the broader public. Lastly, a third layer of transparency includes tailoring the explanation of information to the different types of users of the platform" (Kosters and Gstrein, 2023, p. 130). According to their case study of one VLOP, the DSA contributes to the first two layers through, for example, the provision of information in transparency reports, and to the second layer through the offer of a dashboard for the Statement of Reasons (Digital Services Act, 2024); however, they found that the DSA was still lacking in the third layer of transparency. Ideally, by being able to interlock several different control mechanisms, the forms of transparency that the DSA creates can form a more solid understanding of meaningful, accountable and consistent transparency regimes (Sekwenz and Wagner, 2025, forthcoming).

2.1 A harmonised form of reporting through DSA transparency reports?

The DSA's new rules on transparency reporting can be seen as a predecessor to the provisions that frame reporting under the German NetzDG or the Austrian KoPlG (Heldt, 2019; Werthner et al, 2024, p. 627). According to the DSA, platforms have different reporting obligations to be disclosed in an annual report – or for VLOPs and VLOSEs, in biennial reporting intervals – and such reports must be machine-readable (Art. 15(1) DSA). According to Art. 9 and 10 DSA, transparency reports must include information about orders from public authorities (for example, the police in a Member State), numbers about illegal content or median-time spans of action in response to such notices (Art. 15(1) (a) DSA).

Details provided in transparency reports include data concerning flags received from user-reporting (Art. 16 DSA) describing details of violation reasons, reports from Trusted Flaggers (who report to platforms about illegal content with increased flagging priority, see Art. 22 DSA), the moderation action set (for example, deletion or deplatforming), the automated means included in the moderation process (for instance, the use of Artificial Intelligence (AI) for detecting illegal content) and aspects of reaction time (Art. 15 (1) (b) DSA). Furthermore, details must be included on the specific purpose of the automated means used in the process, their accuracy and the possible error rate of tools like AI (Art. 15(1) (c) DSA). Article 15(1) (d) DSA specifies reporting details on the internal complaint-handling system according to Art. 20 DSA. This mechanism should enable users to question content moderation actions on platforms. The provisions of Art. 24 DSA (see Recital 65 DSA) only apply to online platforms, VLOPs and VLOSEs; these include paragraphs on the out-of-court dispute settlements (Art. 21 DSA), including the number of disputes received, the median time needed to form a decision or the decisions taken in such cases (Art. 24 (1) (a) DSA). In addition, information about malicious user behaviour, such as deplatforming (Kettemann et al, 2022), must be provided according to Art. 23 DSA, for example, details about the reason for suspension (Art. 24 (1) (b) DSA).

Recital 100 opens the scope for Art. 42 DSA, under which "additional transparency requirements should apply specifically to [VLOPs and VLOSEs]" such as biannual reporting obligations. Such platforms must report on the human resources used in the process of content moderation, including details about language skills, educational measures, training or support (Art. 42 (2) (a–b) DSA). Furthermore, Art. 42 DSA requires the inclusion

of qualitative information – broken down to Member State levels (Art. 42 (2) (c) DSA – about the means of content moderation, such as details about the training of content moderators or the educational measures provided to them.

2.2 A place for all platform contracts – The terms and conditions database

According to the DSA, contractual rules governing online behaviour – found in the Community Standards of a platform – are to be provided within the terms and conditions, which are defined in Art. 3 (u) DSA as "all clauses, irrespective of their name or form, which govern the contractual relationship between the provider of intermediary services [the platform] and the recipients of the service [the user]". These and other contractual rules for VLOPs and VLOSEs should be provided in the official languages of all Member State platforms that provide their services and include opt-out details addressed in the generalised contract according to Recital 48 DSA and Art. 14 (6) DSA.

Terms and conditions not only include norms and procedures but also the "measures, and tools" used in content moderation (Art. 14,19 DSA). Since terms and conditions describe how to behave on platforms, these contractual amendments, also referred to as community standards or *netiquette* are a flexible way to adapt frameworks to new challenges, such as the COVID-19 pandemic or wars and conflicts (European Commission, 2022; Kettemann and Sekwenz, 2022). Article 14 DSA requires that users be informed about significant changes (2) and that information is to be provided in a machine-readable format (5). Furthermore, information for children is explicitly mentioned (3), and enforcement has to be in line with fundamental rights (4). Since February 2024, platforms have uploaded their terms and conditions and changes to a website that informs users about the current version that platforms use for content moderation (Terms and Conditions Database, 2024). For the first time, this organised database of contractual rules provides the reader with updates on new clauses, actions or exemptions.

2.3 Quick insights in content moderation decisions through the statement of reason database

The Statement of Reason database is a new measure of transparency in the DSA regulated under Art. 17 DSA. According to Recital 66, "to ensure transparency and to enable scrutiny over the content moderation decisions of the providers of online platforms and monitoring the spread of illegal content online, the Commission should maintain and publish a database which contains the decisions and statements of reasons of the providers of online platforms when they remove or otherwise restrict availability of and access to information". This database therefore captures content moderation decisions in cases of a violation of the terms and conditions (Art. 14 DSA) or the law of a Member State (Art. 3 (h) DSA), similar to the Lumen Database, which was created at Harvard University to capture insight into the moderation process (Lumen Database, 2024). These captured content moderation actions either affect the visibility of content (Art. 17(1) (a) DSA), monetary elements (Art. 17(1) (b) DSA), suspension of the service (Art. 17(1) (c) DSA) or the suspension of an account (Art. 17(1) (d) DSA). Information in the so-called transparency database also includes content moderation decisions such as the facts upon which a decision is based, the circumstances of a case, the source of information (e.g. flagging) or the identity of the notifier (e.g. a Trusted Flagger). Additionally, information about the automated means in the process should be provided as a reference to legal or contractual grounds, as well as information about user rights (e.g. the internal complaint-handling system according to Art. 20 DSA or out-of-court dispute settlements according to Art. 21 DSA). Since the general aim of increasing transparency is welcomed by the community, the accuracy, depth of information and completeness have been critiqued by researchers evaluating the meaningfulness of platforms' reporting practices (Drolsbach and Pröllochs, 2023; Kaushal et al, 2024; Trujillo, Fagni and Cresci, 2024). Such a database is a novum to the world of online governance and opens a path for increased research on platforms to be conducted. The database includes an individual ID for each decision that can be linked to thorough investigations in conjunction with researcher data access or independent audits, and it can also link to the transparency reports of a platform to control for cross-transparency mechanisms (Sekwenz and Wagner, 2025, forthcoming).

2.4 Ad library

Another key database the DSA creates is the advertising repository, the use of which, according to Art. 39 DSA, is mandatory for VLOPs and VLOSEs (Duivenvoorde and Goanta, 2023; Izyumenko et al, 2024). This database provides users with a publicly available search function and API. According to Art. 39(2) (a) DSA, the database should include information about the advertisement (name of the product/service/brand and the subject of the ad, e.g. political advertising). Furthermore, the person on whose behalf the ad is presented has to be disclosed (b–c), in addition to information about the duration of the ad presentation and display (d), targeted and unincluded groups (e–f) and the number of users for whom the ad has been displayed (g). Such information, however, should not be included in the database if the content was classified as illegal under the law of a Member State (Art. 39(3) DSA). Additionally, for the DSA, the upcoming Directive on Transparency and Targeting of Political Advertising will create a new centralised database for this specific type of online advertising at the European level (see Art. 13, Regulation 2024/900).

2.5 Data access for researchers

Article 40 DSA holds specific interest for researchers investigating platforms due to its provision of data access to the DSC or the Commission (Art. 40 (1)). The first part of the Article (1–3) regulates access by public authorities, whereas the second part (4–6 and 8–11) focuses on researcher access. The following section will focus on the second part of Art. 40 due to its relevance for researchers. Research access is provided for the purpose of investigating systematic online risks in order to reduce information asymmetries and support risk mitigation (Kaesling, 2023, p. 639). Therefore, access should be constrained to data concerning the provisions of the DSA, especially understanding and identifying systemic risks according to Art. 35 (Art. 40 (4)).

The DSC can request that VLOPs and VLOSEs "explain the design, the logic, the functioning and the testing of their algorithmic systems" (Art. 40 (3)). Platform providers need to adhere to these requests "within a reasonable period" (Art. 40 (4)); however, platforms can request an amendment to the data access request within 15 days if they do not have access to that data or if the security of their service and trade secrets are endangered

(Art. 40 (5) lit. a–b). The DSC will grant researchers requesting data access the "status of 'vetted researchers' for the specific research" (Art. 40 (8)). These researchers need to fulfil certain requirements as specified in Art. 40 (8) (lit. a-g): researchers must be part of a research organisation (lit. a), which is defined as "a university, including its libraries, a research institute or any other entity, the primary goal of which is to conduct scientific research or to carry out educational activities involving also the conduct of scientific research" (Copyright Directive Art. 2 (1)). The organisation must be non-profit (lit. a) and operate in the public interest (lit. b). Additionally, researchers must work independently and not for commercial interests (lit. b), disclose their research funding (lit. c), protect personal data and implement measures to guarantee data security (lit. d). Furthermore, they must prove that data access is necessary for their research, that it is proportionate and will contribute to the understanding of risk mechanisms (lit. e, f). Finally, researchers must make their results publicly available (lit. g).

Research needs to "contribute to the detection, identification and understanding of systematic risks" (Art. 40(12)). According to Husovec (2023), Art. 40(12) provides two functions: it protects providers against unjust access and minimises technical restrictions of data access for researchers. He argues that scraping should remain central for research aside from API access.

3. On user rights, processes and institutionalised flagging entities

Transparency mechanisms in the DSA combine a variety of different facets of transparency, including transparency reports, the three databases or repositories (terms and conditions, statement of reason and advertising) and the provision of a reporting mechanism for users, as described earlier. On the other hand, the DSA also provides new roles and rights for accredited entities like trusted flaggers, out-of-court dispute settlement bodies and the new legal position of the recipient of a service (see Art. 3 (b) DSA) through the internal complaint-handling system, creating the novel possibility of user empowerment. These mechanisms unfold after the initial content moderation process has ended and open new legal pathways for user empowerment, a more structured response to moderation dissent and the inclusion of experts and civil society on a regular and institutionalised basis (Douek, 2022, pp. 37–51).

3.1 Drop-down of user empowerment? Notice and action mechanisms

Users have been included in the process of content moderation for years and can be described as a central component in the curation of content on platforms such as Reddit or Mastodon (Jhaver et al, 2019; Roth and Lai, 2024). The tool that facilitates user engagement in content moderation is referred to as flagging (Kou and Gui, 2021). The DSA specifies rules on how platforms should design flagging mechanisms in Art. 16 DSA (Sekwenz et al, 2025). A notice action mechanism must empower users to notify the platform about illegal content or contractual violations in a user-friendly design that is easy to access (Art. 16(1) DSA). The design has to indicate the reason why the content has been deemed illegal, a link to the content in question (e.g. URL), the name and email address of the flagging individual and the claim to act in *bona fide* (Art. 16(2) (a-d) DSA). When a user has flagged a piece of content, the intermediary must notify the user (reporting user) about the received notice (Art. 16(4) DSA) as well as the user whose content was reported (Art. 16(5) DSA). Furthermore, Article 16(6) DSA specifies the procedure for platforms to "process any notices that they receive […] and take their decisions in respect of the information to which the notices relate, in a timely, diligent, non-arbitrary and objective manner". Together with the transparency reports of other higher-level means of DSA transparency, the reporting or flagging mechanisms provide a crucial function since they serve as the data collection processes that feed the transparency reports and the statement of reason database. As research on the NetzDG has shown, reporting mechanisms can be used to nudge the user towards reporting loops that favour terms and conditions. As a result, there is more detailed reporting on contractual violations than with the use of the more cumbersome (for the user) illegal content reporting, e.g. through implementing the need to click substantively more often to flag illegal content, leading to low numbers of illegal content flags in transparency reports (Wagner et al, 2020). In 2019, this dark pattern (Brignull, 2019; Gray et al, 2024) of user flagging received a 2 million euros under the German national law in a case brought by national authorities against Facebook (Escritt, 2019).

3.2 Trust me, I am a trusted flagger

Another factor concerning notice action mechanisms in the DSA is the 'fast-lane option' for Trusted Flaggers of illegal content, as specified in

Art. 22 DSA (see Recital 61 DSA; Appelman and Leerssen, 2022). These flaggers have the needed expertise to file flags through the complaint mechanism and, importantly, relevant legal experience that a standard user might not be expected to have.

Trusted Flaggers operate in their "designated area of expertise" when awarded their status after filing an application to the DSC of their Member State (Art. 22(2) DSA; Schwemer, 2019); their status can also be revoked according to Art. 22 (7) DSA). An applicant to the DSC has to fulfil the following conditions: have the expertise and competence to "detect, identify and notify" platforms about illegal content on their service (a), show independence from the platforms (b) and flag "diligently, accurately, and objectively" (c). Flaggers must publish annual reports providing information on their flagging in the relevant time period (Art. 22 (3), Recital 62 DSA); these reports have to be sent to the DSC and made publicly available in a database (Art. 22(5) DSA). The reports should be structured in a way that provides details on the platform the flagging has been applied to (a), the type of illegal content (b) and the platform's moderation action (c). Information and explanation about how the Trusted Flaggers maintain their independence must also be included. Independence mechanisms might include the platforms automatically providing flagging tools for Trusted Flaggers that help to 'book-keep' reported flags from flagging entities. The identity of the Trusted Flaggers is disclosed as well. If a platform observes misbehaviour from Trusted Flaggers, either in submitting "insufficiently precise, inaccurate or inadequately substantiated notices" (Art. 16 DSA) or complaints in the mechanisms provided through the internal complaint-handling system (Art. 20 DSA), the DSC should be informed and after considering evidence and information may suspend the Trusted Flagger (Art. 22(6) DSA). If the investigation into a Trusted Flagger appears to be substantiated (either through the information from a platform or their own initiative), their status can be revoked (Art. 22(7) DSA). In addition, information about notices received by Trusted Flaggers has to be indicated in transparency reports (Art. 15(1) (b) DSA) and can be indicated in the SOR (Art. 17 (3) (b) DSA).

3.3 The wronged user? Internal complaint-handling systems in the DSA

Online platforms, VLOPs and VLOSEs are also obligated to provide an internal complaint-handling system that can be seen as a second step in a platform's reporting or moderation process. Here, a user has the opportunity to use the internal complaint-handling system to lodge complaints about content or accounts for platform decisions within a period of six months (Art. 20 (1) DSA). If a notice received by a platform is not substantiated, the platform can act against the complaint (Art. 20 (3) DSA). Furthermore, this process cannot be fully automated and must have "qualified staff in the loop" of the complaint-handling system (Art. 20 (5) DSA). The question of effective implementation of a complaint-handling system was already questioned in the case of Alibaba in 2024 ('DSA: Commission Opens Formal Proceedings against AliExpress' (European Commission, 2024a).

3.4 The right of a judge or the DSA's answer to it: Out-of-court dispute settlements

After a user has gone through the internal complaint-handling system of a platform, the user still has the right to challenge the content moderation decision: the out-of-court dispute settlement. If a conflict can't be resolved under Art. 20 DSA, the user has the right to "select any out-of-court dispute settlement body that has been certified" according to Art. 21 (1) DSA (Barata, 2023; Coimisiún na Meán, 2024). Such a certification requires mandatory reports; the certified status can also be revoked. According to Art. 21 (3) DSA, redress mechanisms should be easy for users to access to enable them to open a settlement process with an authority in an electronic format. If a case has already been decided, it is not possible for it to be raised again with the dispute settlement body (Art. 21 (2) DSA). Additionally, such a decision does not create binding case law for a platform, as the platform has the freedom to decide similar cases differently. A dispute settlement body must be "impartial and independent, including financially independent" of platforms, have the needed expertise, have a form of remuneration that does not bias the participant in a way that would affect their judgment, be "capable of settling disputes in a swift, efficient and cost-effective manner and in at least one of the official languages", electronically approachable, compliant with the law, apply the rules fairly and have publicly accessible procedures (Art. 21 (3) (a–f) DSA). There currently exist four certified out-

of-court dispute settlement bodies (*ADROIT*, 2024; Europe, 2024; *OPVT*, 2024; *RTR*, 2024; *User Rights*, 2024)

4. In crisis – Please follow the Commission

According to the DSA, a crisis is a situation in which "extraordinary circumstances occur that can lead to a serious threat to public security or public health in the Union or significant parts thereof" (Recital 91 DSA). This rule may have been influenced by the events of the Covid-19 pandemic and was added in quickly following the Russian invasion of Ukraine in February 2022 (Buijs and Buri, 2023; Kettemann and Sekwenz, 2022). Civil society has criticised the subjectivity of the term crisis, the time frames for when a crisis might start or end, the definition of reliable information and the role of human rights in the decision-making process (Access Now, 2022; Coimisiún na Meán, 2024; European Digital Rights, 2024).

When a crisis occurs, the Board adopts a decision to act and the Commission is granted the power to assess the functioning of services, use measures "to prevent, eliminate or limit any such contribution to the serious threat[s]" and be informed about the content in question, the implementation and the impact of the measures demanded (Art. 36 (1) DSA) (Ferreau, 2024). Additionally, the board can issue crisis protocols that provide detailed measures, such as the obligation to display crisis information on platforms (Art. 48 DSA). Crisis protocols can be mandatory or an ex-ante solution for potential crisis situations (Recital 108 DSA).

Any measures implemented by the Commission are bound to certain rules according to Art. 36 (3) DSA, where measures may not exceed a period of three months. Actions need to be "strictly necessary, justified and proportionate" and in line with the Charter of Fundamental Rights; furthermore, clear time frames for measures under the crisis response mechanism must be defined. The DSA requires that decisions to act on a crisis by the Commission be made publicly available, the Board granted the right to access information and provide its views and platforms be immediately informed (Art. 36 (4) DSA). If there is a variety of specific measures, then platforms choose which measure(s) to implement (Art. 36 (5) DSA). Furthermore, the Commission and the platforms should be in dialogue about the implementation, the evaluation of their effectiveness and the goals they seek to achieve (Art. 36 (6) DSA). The Commission must

also report to the EU Parliament and the Council about crisis-response decisions on an annual basis (Art. 36 (11) DSA).

5. Identifying and mitigating systemic risks for intermediaries

The DSA is considered a risk-based Regulation in several aspects of compliance, similar to other EU Regulations such as the GDPR or the AI Act (De Gregorio and Dunn, 2022). The DSA recognises that increased individual and societal risk originates from intermediary services, as many people use these services on a daily basis (Recital 1 DSA). In the DSA, systemic risks are considered in regard to platform functionalities and user behaviour (Brougton Micova and Calef, 2023, p. 6), mixing a top-down and bottom-up approach to risk. Depending on the risks, platforms are required to fulfil a set of obligations (De Gregorio and Dunn, 2022). Search engines were included in the Regulation due to their importance in finding information and maintaining a functioning internet (Kaesling, 2023, p. 533). VLOPs and VLOSEs are required to follow stricter rules due to the increased level of risk associated with such platforms. They are considered to be infrastructures and "de facto public spaces" (Kaesling, 2023, p. 531 transl. by the authors). They need to provide a point of contact for users (Art. 12 DSA), access to the data for the European Commission and for research (Art. 40 DSA) and more transparency (Art. 38, 39, 42). Moreover, external audits are also required (Art. 37). The additional rules that identify more internal processes and measures are defined in Art. 34 and Art. 35 DSA, which will be explained in more detail in the next subsection. Subsequently, the process of external auditing to review the conducted risk assessments will be elaborated.

5.1 That seems pretty risky: Risk assessment under the DSA

According to Art. 34 (1) DSA, VLOPs and VLOSEs need to "identify, analyse and assess" systematic risks once a year (Art. 34(1) S. 2). Systemic risks are not legally defined in the DSA and are only elaborated according to their potential societal impact (Kaesling, 2023, p. 560).

In the following, the Article elaborates on the systemic risks considered in the DSA (Art. 34). First, illegal content (lit. a) is considered to be a high

risk,[5] and the probability of illegal content being distributed on VLOPs and VLOSEs is also considered high (Kaesling, 2023, p. 562).

Subsequently, the legislation mentions "negative effects for the exercise of fundamental rights" (lit. b); these fundamental rights include human dignity, private and family life, the protection of personal data, freedom of expression and information, freedom and pluralism of the media, non-discrimination and the protection of children and consumers (ibid.). One problem concerning fundamental rights – specifically freedom of expression and deliberative democracy – is disinformation (Del Moral Sánchez, 2024, p. 7). Generally, VLOPs and VLOSEs are not obliged to adhere to fundamental rights; however, their position is akin to a public space so their obligation to the public increases (Kaesling, 2023, p. 562f.). The protection of fundamental rights should not lie in the hands of private corporations, and aside from the protection of privacy, fundamental rights were previously not as protected in online spaces compared to the enhanced protection and recognition the DSA provides (Ponce Del Castillo, 2020, p. 3). According to Art. 1 European Charter of Fundamental Rights, the protection of human dignity is critical for the interpretation and application of all other fundamental rights. The protection of human dignity includes the protection against the severe discrimination of vulnerable groups (e.g. due to their sexual orientation) (Borowsky 2019, p. 121), online mobbing and terrorism. In addition, the depiction of child sexual abuse material violates the dignity of children (Kaesling, 2023, p. 563), and denying the Shoah is considered a violation of the dignity of the deceased (Borowsky, 2019, p. 121). Other fundamental rights that are mentioned in Art. 34 lit. b include "respect for private and family life […], the protection of personal data […], freedom of expression and information, including the freedom and pluralism of the media, […] nondiscrimination […], respect for the rights of the child […], and […] a high-level of consumer protection […]".

Furthermore, "negative effects on civic discourse and electoral processes, and public security" (Art. 34 (1)(c), Recital 82) are another risk category. As they are mentioned conjointly, the connection between public debate and electoral processes is emphasised, as these issues may create opportunities that result in danger to public security. Here, information that is not illegal is concerned (Kübler et al., 2023). Social media platforms that are VLOPs

5 For more detailed information on illegal content in the DSA, see Chapter 5 'The Digital Services Act – An Appropriate Response to Online Hate Speech?' by Pascal Schneiders and Lena Auler.

have a responsibility to investigate information interaction that might be part of disinformation campaigns (Kaesling, 2023, p. 567).

Finally, "serious negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being" (Art. 34 (1)(d)) are considered to be a particularly high risk. For such cases, the Commission introduced a threshold wherein the negative effects are required to be *serious*. The seriousness of the consequences is not only considered on a societal level but also regarding the individual persons concerned, including, for instance, the psychological damage to individuals moderating content (Pinchevski, 2023).

Codes of conduct provide guidance for the implementation of risk assessment and mitigation. While the Codes are voluntary, they play a crucial role in risk mitigation and auditing and are therefore considered an "inescapable as part of DSA compliance" (Griffin and Vander Maelen, 2023, p. 4). Examples of Codes of Conduct are the Code on Hate Speech (2016) and the Code of Practice on Disinformation (2018, 2022). The Codes of Conduct apply to consequences of systemic risks such as "disinformation or manipulative and abusive activities" (Recital 103 DSA), including deliberative coordinated efforts to manipulate and mislead, which may be particularly harmful to vulnerable recipients of information. In this regard, following a Code of Conduct is considered risk mitigation measure under Art. 35 DSA (Recital 103 DSA). In 2018, the Code of Practice on Disinformation was developed to encourage self-regulatory behaviours to combat disinformation. However, an assessment of the Code concluded that it was unsuccessful due to a lack of commitment, objectives and tools to measure compliance (Sounding Board, 2018). Therefore, the Strengthened Code of Practice (2022) was developed and is a Code of Conduct under Art. 45 DSA; however, it is still voluntary, complementing the DSA and making it a model of co-regulation. In such a model, the interaction between the intermediary and the regulator is key to its success (Del Moral Sánchez, 2024, p. 17).

5.2 Better to avoid it – Risk mitigation under the DSA

Article 35 DSA proposes risk mitigation measures that intermediaries can employ in case of risk detection. These risk mitigation measures should be "reasonable, proportionate and effective" (Art. 35 (1)). Accordingly, in-

termediaries should be "adapting the design, features or functioning of their services, including their online interfaces" (lit. a) and "adapting their terms and conditions and their enforcement" (lit. b). Furthermore, intermediaries should "test(...) and adapt(...) their algorithmic systems, including their recommender systems (lit. d). According to Art. 8 DSA, there is no proposed general monitoring obligation for platforms and their user-generated content; however, the DSA creates new regulatory rules and practices around content moderation systems. According to the Regulation, content moderation can be understood as:

> [...] the activities, whether 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 (see Art. 14 DSA), provided by recipients of the service, including 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 of the service to provide that information, such as the termination or suspension of a recipient's account. (Art. 3 lit. t DSA)

According to the DSA, content moderation is crucial as a remedy against identified systemic risks on VLOPs and VLOSEs (Art. 35 lit. c); however, if content moderation goes wrong, there can also be negative effects on communities (Feuston et al, 2020).

5.3 Audits

Annual systemic risk assessments are required to be structured in audits that follow the guidelines laid out in the Delegated Regulation (DR) to Art. 27 DSA. These assessments should "diligently identify, analyse and assess any systemic risks in the Union". First, an audit can be conducted on the design or functioning of the service or system, the algorithmic system (see Art. 27 DSA) or the use of the service or system. Second, within these three levels, audits should assess the following factors in their risk assessment (Art. 34 (2) (a-e) DSA):

- the design of their recommender systems and any other relevant algorithmic system,
- the content moderation systems,
- the applicable terms and conditions and their enforcement,

- the systems for selecting and presenting advertisements,
- the data-related practices of the provider.

Within these levels and factors, four categories of risks can be differentiated according to the risks outlined in Art. 34 DSA.

Audits are included in the risk assessment reports (Art. 12(1) DR) and have to follow the inner logic and methodology outlined in the DR (Recital 16, Art. 13(2) (b), Art. 2 (6), Art. 10(4) DR). Audits are not only conducted internally by the platforms according to Art 34 DSA, there is also an external component according to Art. 37 DSA – the independent audit – which is conducted by third parties (e.g. consulting firms) to test the systemic risk assessments of platforms according to Art. 37. External audits also must follow a methodology according to Art. 37 (4) DSA in conjunction with Art. 10 DR and must be filed in a report according to Art. 37(4) DSA. If the audit report does not find the platform's initiatives to act against any risks to have been identified or reported sufficiently, the VLOP or VLOSE in question has to address the auditors' concerns and describe the changes made in an audit implementation report according to Art. 37 (6) DSA.

5.4 The deluge of delegated regulations

Delegated Regulations (DRs) further clarify the DSA. For example, Art. 33 on the definition and calculation of average monthly user numbers to designate VLOPs and VLOSEs is defined in the DR (European Commission, 2023b). Additionally, in Art. 34 and 37, audits are more concisely described and define risk classes for auditing, give guidelines on how to use methodologies and tests to evaluate compliance under the DSA, or give further information on what could be understood under "reasonable level of assurance" DR (European Commission, 2023a). Furthermore, according to Art. 40, the DR on researcher data access outlines how such access should be established, how such accreditation processes should look and how the rights and responsibilities for data access can be distributed. In addition, transparency reports include a DR in their outline to further support coherent reporting process structures and create a guideline to standardise the complex reporting duties in Art. 15, 24 and 42 DSA (European Commission, 2022). Another interesting detail about the DRs in question is that the regulator actively included the feedback of stakeholders and research reports (Wagner et al., 2023) during the process of creating these DRs (*European Commission – Have Your Say*, 2023).

6. Conclusion

To conclude, the DSA introduces a groundbreaking regulatory framework that aims to enhance transparency, accountability and user protection across online platforms, with specific attention focused on VLOPs and VLOSEs. This Chapter has provided an overview of the DSA, one of the first efforts to regulate harmful online content and protect users' fundamental rights online. As discussed in section 2, the DSA's emphasis on transparency is pivotal. The Regulation establishes multiple tools to ensure that platforms are open about their operations, including transparency reports (Art. 15, 24, 42), the Terms and Conditions database (Art. 14), the Statement of Reasons database (Art. 17) and the Ad Library (Art. 39). The novel transparency mechanisms for intermediary services include reports, online repositories (such as the Ad Library according to Art. 39) and Statements of Reason (Art. 17). Furthermore, the DSA provides rules for researchers to access platform data to research systemic risks (Art. 40). The DSA's aims to empower users through new roles and rights, including the Trusted Flaggers mechanism (Art. 22) and the internal complaint-handling system (Art. 20), which reflect the DSA's aim to involve users more actively in content moderation processes by giving them the tools to flag illegal content and challenge platform decisions. Furthermore, the introduction of out-of-court dispute settlements (Art. 21) provides users with a structured and accessible way to seek redress when their rights have been infringed upon. The DSA's includes a crisis response mechanism (Art. 36), which allow the European Commission to rapidly implement measures in extraordinary circumstances such as public health emergencies or threats to public security. These mechanisms, which were influenced by events such as the Covid-19 pandemic and the Russian invasion of Ukraine, provide regulators with the flexibility to act swiftly in times of crisis.

Finally, the DSA adopts a risk-based approach to regulating platforms, particularly VLOPs and VLOSEs, which have a significant societal impact due to their size and reach. The DSA requires these platforms to conduct annual systemic risk assessments (Art. 34) focusing on key areas such as illegal content, infringement of fundamental rights and the protection of minors. Risk mitigation measures (Art. 35) are also mandated, obliging platforms to adapt their systems – recommender algorithms and content moderation processes – to minimise risks to users. Additionally, external audits (Art. 37) are required to ensure that platforms' risk assessments are thorough and that they effectively implement mitigation measures.

In summary, the DSA is a transformative regulation that not only aligns with other EU legislative initiatives, such as the GDPR and AI Act, but also pioneers a new era of platform governance. Its holistic approach, integrating transparency, user empowerment, risk management and crisis response, sets a strong foundation for future digital regulation, aiming to create a safer, fairer and more accountable online ecosystem for all users. As the digital landscape continues to evolve, the DSA's provisions will play a crucial role in ensuring that platforms operate in a manner that respects individual rights and societal values.

References

Access Now (2022) 'Civil Society to EU: Don't Threaten Rights with Last-Minute "Crisis Response Mechanism" in DSA' [Online]. Available at: https://www.accessnow.org/press-release/crisis-response-mechanism-dsa/ (Accessed: 19 July 2024).

Appelman, N. and Leerssen, P. (2022) 'On "Trusted" Flaggers', *Yale Journal of Law & Technology,* 24, pp. 452-475.

Barata J. (2023) 'The Out-of-Court Settlement Mechanism under the DSA: Questions and Doubts', *DSA Observatory* [Online]. Available at: https://dsa-observatory.eu/2023/10/26/the-out-of-court-settlement-mechanism-under-the-dsa-questions-and-doubts/ (Accessed: 19 July 2024).

Bayer, J., Holznagel, B., Lubianiec, K., Pintea, A., Schmitt, J. B., Szakács, J. and Uszkiewicz. E. (2021) 'Disinformation and Propaganda: Impact on the Functioning of the Rule of Law and Democratic Processes in the EU and Its Member States - 2021 Update', PE 653.633. Brussels: European Union.

Borowsky, M. (2019) 'GRCh Art. 1 Würde des Menschen' in Meyer, J. and Hölscheidt, S. (eds.) *Charta der Grundrechte der Europäischen Union,* Baden-Baden: Nomos Verlagsgesellschaft, pp. 81–147.

Broughton Micova, S. and Calef, A. (2023) 'Elements for Effective Systemic Risk Assessment Under the DSA', *SSRN* [Online]. Available at: https://doi.org/10.2139/ssrn.4512640 (Accessed: 9 February 2025).

Bujs, D. and Buri, I. (2023) 'The DSA's Crisis Approach: Crisis Response Mechanism and Crisis Protocols', *DSA Observatory* [Online]. Available at: https://dsa-observatory.eu/2023/02/21/the-dsas-crisis-approach-crisis-response-mechanism-and-crisis-protocols/ (Accessed: 19 July 2024).

Bundesnetzagentur (n.d.) *Digital Services Coordinator* [Online]. Available at: https://www.bundesnetzagentur.de/DSC/DE/_Home/stArt.html (Accessed: 24 May 2024).

Carvalho, J. M., Arga e Lima, F. and Farinha, M. (2021) 'Introduction to the Digital Services Act, Content Moderation and Consumer Protection', *Revista de Direito e Tecnologia,* 3(1), pp. 71–104.

Coimisiún na Meán (2024) 'Article 21 Out-of-Court Dispute Settlement. Guidance and Application Form' [Online]. Available at: https://www.cnam.ie/wp-content/uploads/2024/02/20240216_Article21_GuidanceForm_Branded_vF_KW.pdf (Accessed: 19 July 2024).

Comisiún na Méan (n.d.) 'Online Safety' [Online]. Available at: https://www.cnam.ie/online-safety/ (Accessed: 24 May 2024).

De Gregorio, G. and Dunn, P. (2022) 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age', *Common Market Law Review,* 59(2), pp. 313–26.

De Streel, A., Defreyne, E., Jacquemin, H., Ledger, M. and Michel, A. (2020) *Online Platforms' Moderation of Illegal Content Online. Law, Practices and Options for Reform*, Luxembourg: European Parliament [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf (Accessed: 9 February 2025).

Del Moral Sanchez, M. (2024) 'The DSA and the Fight against Online Disinformation in the Context of EU Law: Avenues for Internal Dialogue and External Territorial Extension', *SSRN Electronic Journal* [Online]. Available at: https://doi.org/10.2139/ssrn.4847475 (Accessed: 26 July 2024).

'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' (2000) *Official Journal of the European Union,* L178, 17 July, pp. 1–16 [Online]. Available at: http://data.europa.eu/eli/dir/2000/31/oj (Accessed; 9 February 2025).

'Directive (EU) 2019/790 of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96 9/ EC and 2001/29/EC' (2019) *Official Journal of the European Union,* L130, May 17, pp. 92–125 [Online]. Available at: http://data.europa.eu/eli/dir/2019/790/oj (Accessed: 9 February 2025).

Dogruel, L., Facciorusso, D. and Stark, B. (2020) '"I'm Still the Master of the Machine." Internet Users' Awareness of Algorithmic Decision-Making and Their Perception of Its Effect on Their Autonomy', *Information, Communication & Society*, 25(9), pp. 1–22.

Drolsbach, C. and Pröllochs, N. (2023) 'Content Moderation on Social Media in the EU: Insights From the DSA Transparency Database', *arXiv*, 7 December [Online]. Available at: http://arxiv.org/abs/2312.04431 (Accessed: 4 February 2024).

Duivenvoorde, B. and Goanta, C. (2023) 'The Regulation of Digital Advertising under the DSA: A Critical Assessment', *Computer Law & Security Review,* 51, 105870 [Online]. Available at: https://doi.org/10.1016/j.clsr.2023.105870 (Accessed: 9 February 2025).

Efroni, Z. (2021) 'The Digital Services Act: risk-based regulation of online platforms', *Internet Policy Review* [Online]. Available at: https://policyreview.info/Articles/news/digital-services-act-risk-based-regulation-online-platforms/1606 (Accessed: 26 July 2024).

Escritt, T. (2019) 'Germany Fines Facebook for Under-Reporting Complaints', *Reuters*, 2 July [Online]. Available at: https://www.reuters.com/Article/us-facebook-germany-fine-idUSKCN1TX1IC (Accessed: 19 August 2023).

European Commission (2016) *Code of conduct on countering illegal hate speech online* [Online]. Available at: 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 (Accessed: 26 July 2024).

European Commission (2018) *Code of Practice Against Disinformation* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation (Accessed: 26 July 2024).

European Commission (2022) *Strengthened Code of Practice on Disinformation* [Online]. Available at https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation (Accessed: 26 July 2024).

European Commission (2023a) *COMMISSION DELEGATED REGULATION (EU) …/… of XXX supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines* [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM:Ares(2023)8428591 (Accessed: 9 February 2025).

European Commission (2023b) *COMMISSION IMPLEMENTING REGULATION (EU) …/… of XXX laying down templates concerning the transparency reporting obligations of providers of intermediary services and of providers of online platforms under Regulation (EU) 2022/2065 of the European Parliament and of the Council* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/delegated-regulation-independent-audits-under-digital-services-act (Accessed: 9 February 2025).

European Commission (2024a) *Commission opens formal proceedings against AliExpress under the Digital Services Act*, Press Release [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_24_1485 (Accessed: 19 July 2024).

European Commission (2024b) *Supervision of the designated very large online platforms and search engines under DSA* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (Accessed: 26 July 2024).

European Digital Rights (2022) *A New Crisis Response Mechanism for the DSA* [Online]. Available at https://edri.org/our-work/public-statement-on-new-crisis-response-mechanism-and-other-last-minute-additions-to-the-dsa/ (Accessed: 19 July 2024).

Ferreau, J. F. (2024) 'Crisis? What Crisis? The Risk of Fighting Disinformation with the DSA's Crisis Response Mechanism', *Journal of Media Law,* 16(1), pp. 57-64.

Griffin, R. and Vander Maelen, C. (2023) 'Codes of Conduct in the Digital Services Act: Exploring the Opportunities and Challenges', *SSRN Electronic Journal* [Online]. https://doi.org/10.2139/ssrn.4463874 (Accessed: 9 February 2025).

Heldt, A. (2019) 'Reading between the Lines and the Numbers: An Analysis of the First NetzDG Reports', *Internet Policy Review*, 8(2) [Online]. Available at: http://policyreview.info/node/1398 (Accessed: 12 July 2019).

Hoboken, J., Buri, I., Quintais, J., Fahy R., Appelman N. and Straub, M. (2023) 'Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications' [Online]. Available at: https://doi.org/10.17176/20230208-093135-0 (Accessed: 9 February 2025).

Hofmann, F. and Raue, B. (2023) 'Einleitung' in Hofmann, F. und Raue, B. (Hrsg.), *Digital Services Act. Gesetz über Digitale Dienste*. Baden-Baden: Nomos, pp. 32–48.

Husovec, M. (2023) 'How to Facilitate Data Access under the Digital Services Act', *SSRN* [Online]. Available at: https://ssrn.com/abstract=4452940 (Accessed: 26 July 2024).

Iosifidis, P. and Nicoli, N. (2021) *Digital Democracy, Social Media and Disinformation*. London: Routledge.

Izyumenko, E., Senftleben, M., Schutte, N., Smit, E. G., van Noort, G. and van Velzen, L. (2024) 'Online Behavioural Advertising, Consumer Empowerment and Fair Competition: Are the DSA Transparency Obligations the Right Answer?', *SSRN* [Online]. Available at: https://papers.ssrn.com/abstract=4729118 (Accessed: 21 May 2024).

Jhaver, S., Birman, I., Gilbert, E. and Bruckman, A. (2019) 'Human-Machine Collaboration for Content Regulation: The Case of Reddit Automoderator', *ACM Transactions on Computer-Human Interaction*, 26(31), pp. 1–35.

Just, N. and Saurwein, F. (2024) 'Enhancing Social-Media Regulation through Transparency? Examining the New Transparency Regime in the EU', *TechREG Chronicle,* 2 [Online]. Available at: https://www.zora.uzh.ch/id/eprint/257668 (Accessed: 21 May 2024).

Kaesling, K. (2023) 'Zusätzliche Verpflichtungen in Bezug auf den Umgang mit systemischen Risiken für Anbieter von sehr großen Online-Plattformen und sehr großen Online-Suchmaschinen', in Hofmann, F. und Raue, B. (eds.), *Digital Services Act. Gesetz über Digitale Dienste*. Baden-Baden: Nomos. DSA Kommentar, pp. 631–684.

Kapantai, E., Christopoulou, A., Berberidis, C. and Peristeras, V. (2021) 'A Systematic Literature Review on Disinformation: Toward a Unified Taxonomical Framework', *New Media & Society*, 23(5), pp. 1301–26.

Kaushal, R., van de Kerkhof, J., Goanta, C., Spanakis, G. and Iamnitchi, A. (2024) 'Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database', *Arxiv,* 3 May 2024 [Online]. Available at: http://arxiv.org/abs/2404.02894 (Accessed: 9 April 2024).

Kettemann, M.C. and Sekwenz, M.T. (2024) 'Pandemics and Platforms: Private Governance of (Dis)Information in Crisis Situations', in Kettemann, M.C., Lachmayer, K. (ed.). *Pandemocracy in Europe.* Oxford: Hart Publishing, pp. 263–282.

Kou, Y. and Gui, X. (2021) 'Flag and Flaggability in Automated Moderation; The Case of Reporting Toxic Behavior in an Online Game Community', *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems,* Article 437, pp. 1–12. Association for Computing Machinery [Online]. Available at: https://doi.org/10.1145/3411764.3445279 (Accessed: 24 June 2024).

Kübler, J., Sekwenz, M. T., Rachinger, F., König, A., Gsenger, R., Pirkova, E., Kettemann, M.C., Wagner, B., Krennerich, M. and Ferro, C. (2023) 'The 2021 German Federal Election on Social Media: Analysing Electoral Risks Created by Twitter and Facebook', *Proceedings of the 56th Hawaii International Conference on System Sciences,* 56, pp. 4036–4045.

Murray, J. and Flyverbom, M. (2020) 'Datafied Corporate Political Activity: Updating Corporate Advocacy for a Digital Era', *Organization,* 28(4), pp. 621–640.

Pinchevski, A. (2023) 'Social Media's Canaries: Content Moderators between Digital Labor and Mediated Trauma', *Media, Culture & Society,* 45(1), pp. 212–21.

Ponce Del Castillo, A. (2020) 'The Digital Services Act Package: Reflections on the EU Commission's Policy Options', *ETUI Policy Brief. European Economic, Employment and Social Policy,* 12 [Online]. Available at: https://www.etui.org/sites/default/files/2020-09/The%20digital%20services%20act%20package.%20Reflections%20on%20the%20EU%20Commission%27s%20policy%20options-2-2020.pdf (Accessed: 9 February 2025).

'Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act)', *Official Journal of the European Union*, 65 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:277:FULL&from=EN (Accessed: 26 July 2024).

Rodríguez De Las Heras Ballell, T. (2021) 'The Background of the Digital Services Act: Looking towards a Platform Economy', *ERA Forum,* 22(1), pp. 75–86.

Roth, Y. and Lai, S. (2024) 'Securing Federated Platforms: Collective Risks and Responses', *Journal of Online Trust and Safety,* 2(2) [Online]. Available at: https://tsjournal.org/index.php/jots/Article/view/171 (Accessed: 4 March 2024).

Schwemer, S. F. (2019) 'Trusted Notifiers and the Privatization of Online Enforcement', *Computer Law & Security Review,* 35(6), 105339 [Online]. Available at: https://doi.org/10.1016/j.clsr.2019.105339 (Accessed: 9 February 2025).

Schwemer, S. F. (2023) 'Digital Services Act: a reform of the e-Commerce Directive and much more', in Savin, A. and Trzaskowski, J. (eds.) *Research Handbook on EU Internet Law*. Cheltenham: Elgar, pp. 232–253.

Sounding Board (2018) 'The Sounding Board's Unanimous Final Opinion on the So-Called Code of Practice', 24 September 2018 [Online]. Available at: https://www.ebu.ch/files/live/sites/ebu/files/News/2018/09/Opinion%20of%20the%20Sounding%20Board.pdf (Accessed: 26 July 2024).

Trujillo, A., Fagni, T. and Cresci, S. (2024) 'The DSA Transparency Database: Auditing Self-Reported Moderation Actions by Social Media', *arXiv*, 20 January 2024 [Online]. Available at: http://arxiv.org/abs/2312.10269 (Accessed: 9 February 2024).

Wagner, B., Rozgonyi, K., Sekzwenz, M. T., Cobbe, J. and Singh, J. (2020) 'Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act', *Association for Computing Machinery, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* [Online]. Available at: https://doi.org/10.1145/3351095.3372856 (Accessed: 22 August 2021).

Werthner, H., Ghezzi, C., Kramer, J. et al (eds) (2024) *Introduction to Digital Humanism: A Textbook*. Berlin: Springer Nature Switzerland.