Digital Services Act: A reform of the e-Commerce Directive and much more

Schwemer, Sebastian Felix

Publication date: 2022

Citation for published version (APA):
Digital Services Act:
A reform of the e-Commerce Directive and much more

Sebastian Felix Schwemer\textsuperscript{12}

I. BACKGROUND AND LEGISLATIVE HISTORY OF THE DSA

Long gone are the heydays of a more static internet with GeoCities, Myspace, hand-curated link lists and the likes. Much has happened since the early days of the “information superhighway” over twenty years ago.\textsuperscript{3} Over recent years, public scrutiny turned towards the multiple unresolved issues regarding large online platforms’ role in society and their power.\textsuperscript{4} During the last five years or so, the EU lawmaker, too, has increasingly focused on addressing the complex issues around the governance of (illegal) information on the internet and the role of private internet intermediaries - most notably of large online platforms.

A variety of sector-specific legislative and soft law instruments has been introduced, such as the infamous Article 17 of the Directive on copyright in the Digital Single Market\textsuperscript{5}, the Regulation for terrorist content\textsuperscript{6} or the Commission’s Recommendation on measures to effectively tackle illegal content online\textsuperscript{7} (and earlier Communication).\textsuperscript{8} In parallel, the EU lawmaker has worked with co-regulation in this area, through efforts such as the Code of Practice on Disinformation and the EU Code of Conduct on Countering Illegal Hate Speech Online. These initiatives have been accompanied by legislative initiatives to tackle illegal online content at national level, including in non-harmonized areas of EU law like hate speech, e.g., in Germany, Austria and France.

\textsuperscript{1} Associate Professor, Centre for Information and Innovation Law (CIIR), University of Copenhagen, and Adjunct Associate Professor, Norwegian Research Center for Computers and Law (NRCCL), University of Oslo. E-mail: sebastian.felix.schwemer@jur.ku.dk.
\textsuperscript{2} The author has been involved in preparatory works and was \textit{inter alia} main author of one of the two background studies commissioned by DG Connect in preparation of the DSA. See SF Schwemer, T Mahler and H Styri, \textit{Legal analysis of the intermediary service providers of non-hosting nature} (Final report prepared for European Commission, 2020), <https://data.europa.eu/doi/10.2759/498182>. Parts of this research are part of the reCreating Europe project, which has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 870626.
\textsuperscript{3} European Commission, Green Paper 1995 Copyright and related rights in the information society, COM (95) 382 final.
\textsuperscript{4} E.g. Wallstreet Journal’s ‘Facebook Files’, the Christchurch attack In New Zealand or information quality during the Covid-19 pandemic.
\textsuperscript{8} For an overview, see, T Riis and SF Schwemer, “Leaving the European safe harbor, sailing towards algorithmic content regulation” 22(7) \textit{Journal of Internet Law}, 1-21.
Against this background, the Digital Services Act (DSA) represents a shift in the EU’s approach. It is the first overhaul of the horizontal rules of the e-Commerce Directive9, which since the early 2000s constituted the EU law cornerstone and centerpiece regulating the principles of the role and responsibilities of internet intermediaries. For more than two decades the e-Commerce Directive’s Chapter II on Principles, Section 4 on the “Liability of intermediary service providers”10 contained fundamental principles of whether and when internet intermediaries may be held liable for illegal information/content provided by third parties.

Over the last decade, the role of internet intermediaries in the governance of information on the internet has grown significantly more important. Notably, (very-large) online platforms employ various content moderation and content recommendation methods. Increasingly, these methods include automation and algorithmic solutions aimed at detecting and moderating various types of content, for example intellectual property (especially copyright), hate speech, terrorist content, as well as harmful content (such as misinformation or “lawful but awful” content). Academic research from various disciplines as well as policy making have identified multiple often interrelated issues surrounding this privatization of enforcement, which was not foreseen by the drafters of the e-Commerce Directive in the late 1990’s in this scale. Whereas the original objectives of the e-Commerce Directive remain valid, the Commission had preliminary identified several issues that demand an updating, namely: the change of scale and diversity in the use of digital services since 2000, emerging legal fragmentation and challenges regarding enforcement and oversight of digital services.11

Figure 1: Timeline

---


10 The title of the Chapter should not be misunderstood: the question of liability is, with a few exceptions such as copyright in the context of Art. 17 CDSM Directive where liability is harmonised on the EU-level, first and foremost determined according to national standards, such as the Danish “medvirkensansvar” or the German “Störerhaftung”. The ECD’s rules, in turn, regulate the exemption of such liability.

Fast forward, on 15 December 2020, the European Commission presented its highly anticipated proposal for a Regulation on a Single Market For Digital Services\(^\text{12}\) coined the Digital Services Act (DSA) as part of its Digital Services package.\(^\text{13}\) On 5 July 2022, the European Parliament passed the DSA in first reading with a broad majority.\(^\text{14}\) At the time of this writing, the Council vote is still outstanding but following the trilogue agreement considered mere formality. Effectively, the DSA will have moved from proposal in late 2020 to adopted Regulation sometime in Q3/Q4 2022, i.e., in less than two years.

This speedy process is evidence of the EU bodies’ sense of urgency and falls in a time of extreme regulatory activity.\(^\text{15}\) But it is also testament to the legislative process, which started long before the Commission’s official proposal. In November 2019, then Commission President Elect Ursula von der Leyen put the Digital Services Act, which “will upgrade our liability and safety rules for digital platforms, services and products, and complete our Digital Single Market”\(^\text{16}\) high on her political guidelines and concomitantly on the political agenda in Brussels.

Even before that an internal working document of the Unit Online Platforms & eCommerce at the Directorate-General for Communication Networks, Content and Technology (DG Connect) explored a potential opening and updating of the e-Commerce Directive. In July 2019, by accident, this document was leaked.\(^\text{17}\) In the immediate aftermath of the widely reported leak, both European institutions, Member States as well as various stakeholders started engaging in this dialogue.\(^\text{18}\) Thus, this mishap, one could argue, has helped the speedy adoption process: Effectively, many discussions around how the future of the e-Commerce Directive’s liability exemption rules should look like and how to tame big tech and their algorithmic influence over society, be it through content moderation or recommendation, was “frontloaded” before the Commission’s inception impact assessment and public consultation in the summer of 2020. In November 2019, for example, an “Information from the Commission and exchange of views” was scheduled by the Council\(^\text{19}\), while the European Parliament (IMCO, JURI, LIBE committees) started preparing multiple initiative

---


\(^{14}\) 539 votes in favour, 54 votes against, 30 abstentions.

\(^{15}\) Besides DSA and DMA, e.g., proposals for Data Act, Data Governance Act, Digital Content Directive, Terrorist Content Regulation, Child sexual abuse (CSAM) regulation, CDMS Directive, Artificial Intelligence Act.


\(^{19}\) Council of the European Union, Notice of Meeting and Provisional Agenda, Joint working party on telecommunications and information society / competitiveness and growth (internal market), Brussels, 25 October 2019, <https://www.parlament.gv.at/PAKT/EU/XXVII/EU/00/03/EU_00364/index.shtml> (last accessed 10 August 2022).
reports due in the first half of 2020. The D9+ countries issued their non-paper, the tech companies’ interest organisation EDIMA published its position paper suggesting a new “Online Responsibility Framework” and so on. All those developments took place before Commissioners Vestager and Breton presented their proposal on 15 December 2020.

After the comprehensive proposal, comprising of 106 recital and 74 articles, the Brussels bubble kept busy and the Commission’s text was subject to fierce lobbying by stakeholders and substantive amendments in the legislative process. A detailed account of developments, however, would go far beyond the purpose of this chapter. The trilogue, an utterly opaque but central process, was concluded in the early hours of 23 April 2022 under the French Council presidency. Unless otherwise expressed, this chapter is based on the text of the Digital Services Act adopted in first reading at the European Parliament on 5 July 2022. Numbering of recitals and articles may be subject to technical adjustments in the further process before publication in the Official Journal, whereas substantive changes cannot occur. The bulk of provisions in the DSA is expected to enter into force on 1 January 2024. So, what is new under the sun?

II. ONE ACT, MULTIPLE PROTAGONISTS: THE LEGAL DESIGN OF THE DSA

The legal design of the DSA is as follows: Firstly, it preserves (cf. recital 16 DSA) and updates the ECD’s liability exemptions for third-party (i.e., user-uploaded content) for internet intermediaries (or more specifically, the providers of functions of “mere conduit”, “caching” and hosting). As a novelty, these principles will be enshrined in a Regulation (vis-à-vis the previous Directive) and thus apply directly in EU and EEA Member States without the need for (or discretion in) implementation.

28 D9+ NON-PAPER ON THE CREATION OF A MODERN REGULATORY FRAMEWORK FOR THE PROVISION OF ONLINE SERVICES IN THE EU (May 2020).
22 Suffice it to note that, inter alia, the so-called Schaldemose-Report (IMCO) has been central to the discussion with many notable amendments, including, e.g., a 24-hour time deadline to remove content, see European Parliament, “REPORT on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC”, 20.12.2021 - (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)), Rapporteur: Christel Schaldemose.
25 See Art. 74 DSA.
26 Cf. Art. 1(1) DSA.
27 Note the quotation marks in Arts. 12 and 13 ECD and correspondingly in Arts. 3 and 4 DSA.
28 Art. 15 ECD represents the cornerstone of the fundamental rights balance on the internet; Denmark, for example, never implemented the provision in its national law “echandeloven” with the argument that the national implementation in fact does not lead to general monitoring. Given the legal instrument – a regulation vis-à-vis Directive – there will be no need for implementations.
Secondly, the DSA introduces a “whole new regulatory layer”\(^29\), namely a novel set of asymmetric due diligence obligations for providers of intermediary services. Importantly, these due diligence obligations are separate from the question or availability of a liability exemption\(^30\) and build upon and codify many aspects of the Commission’s Recommendation from 1 March 2018.

Lastly, this system of due diligence obligations is accompanied by a new partly de-centralised enforcement system, which will not be explored in detail here. Clearly inspired by the General Data Protection Regulation\(^31\), it leaves direct supervision and enforcement to national competent authorities\(^32\) and Digital Services Coordinators designated by Member States and introduces a European Board for Digital Services (EBDS)\(^33\) for coordination purposes. It is especially noteworthy that the Commission is entrusted with special competences as enforcement body notably in relation to very large online platforms and search engines\(^34\). Non-compliance can in certain instances be fined with up to 6 % of annual worldwide turnover\(^35\), a notch higher than the 4 % fines under the GDPR. The Commission and the Joint Research Centre also plan to establish a European Centre for Algorithmic Transparency. A deeper analysis of this regime, however, is outside the scope of this chapter.

Speaking of scope, the geographic scope of the DSA is broad. According to Article 1a (1) DSA, it applies to “intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of the place of establishment of the providers of those services.” This extraterritorial effect is deemed necessary to ensure a “level playing field” and the effectiveness of the rules (recital 7 DSA). Recital 7 DSA further brings forward a requirement of “substantial connection”, which in the absence of an EU establishment is to be considered when such intermediary service has a significant number of users in the EU or targets its activities towards a Member State, e.g., by using a relevant top-level domain name (recital 8 DSA).

The material scope of the DSA, too, is broad. The e-Commerce Directive’s liability exemption rules formed the very fundamentals of EU internet (content) regulation. This is manifested by the relative technological neutrality of the ECD’s rules\(^36\) and by the double horizontal nature of the framework. Articles 12-14 ECD shield from any form of liability (administrative, civil and criminal) and do not discriminate between specific forms of content. Similarly for the DSA, recital 17 notes: “exemptions from liability established in this Regulation should apply in respect of any type of liability as regards any type of illegal content, irrespective of the precise subject matter or nature of those laws.”\(^37\)


\(^30\) See in detail below.


\(^32\) In Norway, for example, the national Data Protection Authority Datatilsynet has publicly shown great interest in the DSA, whereas the e-Commerce Directive is currently under the NKOM agency.

\(^33\) Compare this setup also to the European Data Protection Board (EDPB) in the GDPR or the European Artificial Intelligence Board (EAIB) in the proposed AI Act.

\(^34\) Art. 44a (1a) and (1b) DSA.

\(^35\) Arts. 42(3), 59(1) DSA; note also the possibility for periodic penalty payments, Art. 60 DSA.

\(^36\) See, however, Schwemer, Mahler and Styri (2020) on potential technological limits.

\(^37\) See also the definition of illegal content in Art. 2(g) DSA meaning “any information, which, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the
Thus, at its starting point, the DSA does not stretch into regulating “harmful” or “lawful but awful” content.\textsuperscript{38}

While the majority of public and political attention focusses on (very-large) online platforms such as Facebook, Youtube, TikTok, GitHub, Pornhub, Amazon and similar, the DSA addresses all providers of so-called intermediary services, in other words, the whole internet intermediary “stack”. This includes notably infrastructure-related functions “mere conduit” and “caching”. Both from a technical, business and fundamental rights perspective, the role that these non-hosting intermediaries play is different from online platforms.\textsuperscript{39} In order to avoid spill-over effects, e.g., from the content moderation debate regarding online platforms, it is therefore essential to be aware of their differences and particularities.

III. OVERHAUL OF THE LIABILITY EXEMPTION PRINCIPLES: NOTHING NEW UNDER THE SKY? OH, WAIT!

The e-Commerce Directive’s conditional liability exemption framework has despite fast-paced developments generally worked well and is preserved. The DSA notes, however, that “in view of the divergences when transposing and applying the relevant rules at national level, and for reasons of clarity and coherence, that framework should be incorporated in this Regulation” (recital 16). Furthermore, it was deemed “necessary to clarify certain elements of that framework, having regard to case law” of the CJEU (recital 16).

At its outset, the legal design of the liability exemptions from the e-Commerce Directive remains unchanged. Basically, Articles 12-15 e-Commerce Directive in Chapter II on Principles, Section 4 on the “Liability of intermediary service providers” are transferred almost verbatim to Chapter II of the DSA on the “Liability of providers of intermediary services”.\textsuperscript{40} Thus, the DSA continues the function-oriented approach with conditional horizontal liability exemptions for ‘mere conduit’, ‘caching’ and hosting accompanied by the prohibition of (mandated) general monitoring. It is important to underscore, however, that the liability exemption framework will be contained in a Regulation (Article 288 TFEU) and thus directly applicable without Member States’ implementation (and potential discretion\textsuperscript{41}).

\textsuperscript{38} At the same time, however, certain aspects tinker into these grounds, notably risk mitigation mechanisms for VLOPs, see below. See also M Huosvec and I Roche Laguna, “Digital Services Act: A Short Primer” (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4153796> 11
\textsuperscript{39} This concern is aggravated by the fact that legal scholars seem to overlook that already the ECD covered more than hosting, see, e.g., AP Heldt, “EU Digital Services Act: The White Hope of Intermediary Regulation”, in: T Flew & F Martin (ed) Digital Platform Regulation: Global Perspectives on Internet Governance (Palgrave Macmillan, 2022) 72.
\textsuperscript{40} See also Art. 71(1) and (2) DSA.
The devil, however, is in the detail and there are a several noteworthy changes both in provisions as well as recitals – partly already suggested by the European Commission in its proposal, partly amended or introduced later in the legislative process–, which will have to be examined in detail in the future to fully understand the “updated” liability exemption framework established by the DSA.

A. ‘MERE CONDUIT’, ‘CACHING’ AND HOSTING: MINOR TWEAKS TO THE PROVISIONS

Whereas the liability exemption conditions for ‘mere conduit’ services remain unaltered, Article 3 DSA (ex-Article 12 ECD) adds that that the service provider is not liable for the “information transmitted or accessed”. Similarly, the provision on ‘caching’ (Article 4 DSA, ex-Article 13 ECD) remains largely unchanged, however, with the noteworthy addition that the sole purpose of such service may also consist in making the onward transmission “more secure”. Also the liability exemption for hosting, formerly Article 14 e-Commerce Directive, has been subject to changes, namely that “illegal information” has been replaced with “illegal content” in Article 5 DSA; presumably of a merely cosmetic nature. More significantly, the hosting liability exemption in the DSA does not apply to e-commerce online platforms /online marketplaces under certain conditions with respect to liability under consumer protection law according to Article 5(3) DSA. Finally, despite various suggestions for amendments, also Article 15 e-Commerce Directive is transferred – in line

Table 1: Comparison between e-Commerce Directive and Digital Services Act

<table>
<thead>
<tr>
<th>e-Commerce Directive</th>
<th>Digital Services Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 12 – “Mere conduit”</td>
<td>Article 3 – ‘Mere conduit’</td>
</tr>
<tr>
<td>Article 13 – “Caching”</td>
<td>Article 4 – ‘Caching’</td>
</tr>
<tr>
<td>Article 14 – Hosting</td>
<td>Article 5 – Hosting</td>
</tr>
<tr>
<td>Article 15 – No general obligation to monitor</td>
<td>Article 6 – Voluntary own-initiative investigations and legal compliance</td>
</tr>
<tr>
<td>Article 13 ECD</td>
<td>Article 7 – No general monitoring or active fact-finding obligations</td>
</tr>
<tr>
<td>Article 14 ECD</td>
<td>Article 8 – Orders to act against illegal content</td>
</tr>
<tr>
<td>Article 15 ECD</td>
<td>Article 9 – Orders to provide information</td>
</tr>
</tbody>
</table>

42 Arts. 8 and 9 DSA will not be analysed in detail here. Suffice it to note that they introduce concrete obligations to act against illegal content and set forth procedural requirements.
43 The new enforcement mechanism for national authorities in Arts. 8 and 9 DSA will not be analysed further in this chapter.
44 i.e. Art. 12 ECD, Art. 3 DSA.
45 Emphasis added on the addition compared to ECD.
46 i.e. Art. 13 ECD, Art. 4 DSA.
47 This addition can, for example, be relevant in the context of Content Delivery Networks.
48 Namely in instances where an average consumer would believe “that the information, or the product or service that is the object of the transaction, is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control.”
with the Commission’s proposal from December 2020– with merely technical changes to Article 7 DSA on ‘No general monitoring or active fact-finding obligations’. As a novelty, recital 28 DSA adds in this context that this prohibition concerns both de jure and de facto general monitoring obligations.

B. RECITALS: GOING BEYOND MERE CLARIFICATIONS?

A more nuanced and complex picture regarding the continuation of the three liability exemptions emerges when taking into account the corresponding recitals in the preamble. Historically, recitals of the e-Commerce Directive have played an important role in the CJEU’s jurisprudence. One basic prerequisite for the availability of liability exemptions is the passive role of the respective service provider. Under the e-Commerce Directive regime, the liability exemption is limited to activities, which are ‘of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.’ In its case law, the CJEU extended this prerequisite from ‘mere conduit’ and ‘caching’ to hosting. Over the years, however, it has been asked whether this criterion is useful in the first place in light of increasing automation activities. The Commission’s leaked concept note predating the DSA proposal from 2019 remarked that ‘(...) the concept of active/passive hosts would be replaced by more appropriate concepts reflecting the technical reality of today’s services, building rather on notions such as editorial functions, actual knowledge and the degree of control.’

The Court’s jurisprudence on the matter, in any case, is now codified in recital 18 DSA, which clarifies that the ‘exemptions from liability established in this Regulation should not apply where, instead of confining itself to providing the services neutrally, by a merely technical and automatic processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information.’ Thus, whereas the Commission had contemplated abandoning the concept altogether

---

50 This observation may very well not become relevant but note that Art. 7 DSA refrains from directly referencing back to Arts. 3 to 5 DSA and instead regards ‘the information which providers of intermediary services transmit or store’ (emphasis added). Since Art. 3 DSA (‘mere conduit’) also refers to “information accessed”, this function may in a strict textual reading fall outside the scope of the ban on general monitoring in Art. 7 DSA; such interpretation, however, can hardly be read into the intention of the legislator.

51 Recital 42 ECD.

52 See, e.g., C-324/09, L’Oreal and Others, ECLI:EU:C:2011:747, para. 113; C-236/08 to C-238/08, Google France and Google, ECLI:EU:C:2010:159, para. 113; C-291/13, Papasavvas, ECLI:EU:C:2014:2299, paras. 40 ff.; see, however, also opposing view by AG in C-324/09, L’Oreal and Others, Opinion of Advocate General Jääskinen, ECLI:EU:C:2010:757, paras. 138–142.


54 The recital continues “[t]hose exceptions should accordingly not be available in respect of liability relating to information provided not by the recipient of the service but by the provider of the intermediary service itself, including where the information has been developed under the editorial responsibility of that provider.”
and replace it with other concepts, the DSA now codifies the case law without further specifying the active/passive distinction.

Speaking of the Court, whereas the CJEU’s –relative sparse but growing body of– on Articles 12 to 15 eCommerce Directive is not directly applicable to the DSA’s rules in Articles 3 to 7 DSA, the Court’s interpretations should, where still relevant, remain their validity where provisions have not been altered substantially or altered only for cosmetic reasons.55

In the DSA, in any case, the legislator has turned towards recitals as central mechanism for clarifying and updating the 22-year-old intermediary liability framework, to the detriment of a more substantive revision.56 Recital 17 DSA, for example, contains the –probably redundant but– welcome reminder that the DSA’s liability exemption rules are not to be “be understood to provide a positive basis for establishing when a provider can be held liable, which is for the applicable rules of Union or national law to determine”.57 Another more principal systematic clarification is contained in recital 26 DSA, which reminds that third parties should resolve conflict without involving the intermediary, and in case such involvement is necessary clarifies a proportionality principle according to which “any requests or orders for such involvement should, as a general rule, be directed to the specific provider that has the technical and operational ability to act against specific items of illegal content, so as to prevent and minimise any possible negative effects on the availability and accessibility of information that is not illegal content”. Concomitantly, more remote intermediaries should only be targeted as a last resort.58 Furthermore, the DSA’s recitals also contain further substantive clarifications which update and adjust the ECD’s framework.

Holistic internet regulation: (auxiliary) intermediary services and the world beyond platforms

An important principal question that has received only relatively limited attention concerns the availability of liability exemptions for more remote, technical intermediary functions and intermediary services that are not in the political “spotlight”: Due to the wording of Articles 12 and 13 eCommerce Directive and the character of the legal instrument as Directive, it has been unclear whether, e.g., providers of DNS or CDN services would benefit from one of the liability exemptions. Whereas the European legislator refrained from introducing a fourth category for auxiliary intermediary services as suggested by Schwener, Mahler and Styri (2020)59, recital 27 (and recital 27a) clarifies that “providers of services establishing and facilitating the underlying logical architecture and proper functioning of the internet, including technical auxiliary functions”, too, can benefit from the DSA’s liability exemptions. Importantly in this context recital 27a provides a non-exhaustive list of examples of “generic” intermediary services (Table 2 below). Furthermore, the recital reflects on the fact that such services “may be provided in isolation, as a part of another type of intermediary service, or simultaneously with other intermediary services” and that its categorization solely depends on its technical functionality.

---

55 See in this vein also Art. 71(2) DSA, stating “References to Articles 12 to 15 of Directive 2000/31/EC shall be construed as references to Articles 3, 4, 5 and 7 of this Regulation, respectively”.
56 See, e.g. proposal the proposal to introduce a category of “auxiliary network intermediary” functions as proposed by Schwener, Mahler and Styri (2020), 60 f.
57 A prominent example of such harmonised liability on the EU-level is within the field of copyright with Art. 17(1) CDSM Directive.
58 Similarly suggested by Schwener, Mahler and Styri (2020), 61.
Table 2: Examples of “generic” intermediary services in recital 27a DSA

<table>
<thead>
<tr>
<th>‘mere conduit’ intermediary services</th>
<th>‘caching’ intermediary services</th>
<th>‘hosting services’</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 2(f) (i) DSA: “(...) consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network,”</td>
<td>internet exchange points, wireless access points, virtual private networks, DNS services and resolvers, top-level domain name registries, registrars, certificate authorities that issue digital certificates, voice over IP and other interpersonal communication services</td>
<td>content delivery networks, reverse proxies or content adaptation proxies</td>
</tr>
<tr>
<td>Art. 2(f) (ii) DSA: “(...) consists of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information’s onward transmission to other recipients upon their request,”</td>
<td></td>
<td>cloud computing, web hosting, paid referencing services or services enabling sharing information and content online, including file storage and sharing</td>
</tr>
</tbody>
</table>

**Actual knowledge considering increased automation by platforms**

Another tricky question in the context of hosting (Article 5 DSA, ex-Article 14 ECD) relates to the criterion of “actual knowledge” against the background of commonplace automatic activities “such as tagging, indexing, providing search functionalities, or selecting content” and to what extent those could be construed to give actual knowledge. Already the Commission’s Impact Assessment noted that such activities are necessary features from an UX-perspective and furthermore “are absolutely necessary to navigate among an endless amount of content” and therefore should not be considered a “smoking gun.” In this vein, recital 22 DSA now clarifies that actual knowledge “cannot be considered to be obtained solely on the ground that the provider is aware, in a general sense, of the fact that its service is also used to store illegal content”. It names specifically automated indexing, search functions and recommendations “on the basis of the profiles or preferences of the recipient” as activities, which do not establish ‘specific knowledge’ in the sense of Article 5(2) DSA.

---

60 Note a slight – arguably cosmetic – difference in wording compared to the liability exemption in Art. 3(1) DSA.  
61 Note the lacking purpose of making a transmission more “secure”, compared to the liability exemption in Art. 4(1) DSA.  
62 DSA Impact Assessment – Part 2/2 (Brussels, 15 December 2020) SWD(2020) 348 Final, 159; see also background study to DSA by Hoboken et al. (2019), 37 ff.  
C. A (SOMETHING) GOOD SAMARITAN PROVISION

The legislator also opted for a regulatory novelty with the introduction of a so-called Good Samaritan clause in Article 6 DSA on “Voluntary own-initiative investigations and legal compliance”. The concept, borrowed from the parable of the Good Samaritan in the bible, has been used in a legal context primarily in Common Law traditions. The European Commission, in any case, understands “proactive steps to detect, remove or disable access to illegal content” as such Good Samaritan actions. Already in 2017, the Commission flagged this idea as a response to the incentive problem, which intermediaries (or, more specifically, very-large online platforms) apparently face: voluntarily introducing proactive (algorithmic) measures to detect illegal information could be seen as indication that the provider is not merely passive and thus falling out of the applicability of the liability exemption. Despite this interpretation never being tested before the CJEU, despite the commonplace practice of proactive content moderation by platforms and despite the Commission putting forward their interpretation e.g. in Recommendation 2018, several online platforms argued for the introduction of such a clarification. According to the provision in Article 6 DSA, in any case, providers of intermediary services do not lose their liability exemption “solely because they, in good faith and in a diligent manner, carry out voluntary own-initiative investigations or take other measures aimed at detecting, identifying and removing, or disabling of access to, illegal content” or for compliance reasons.

Whereas this provision has been primarily discussed with (very-large) online platforms like Facebook, Instagram or Youtube in mind, it is noteworthy that Article 6 DSA indeed applies to all intermediaries including internet access service providers or caching services. Therefore, the proportionality of such voluntary measures might become a central question. The provision refrains from further specifying what would qualify as such “voluntary” action. Since the European lawmaker has for platform regulation often relied on soft law and co-regulation (in addition to or in lieu of hard law enacted by institutions), e.g., by facilitating codes of conduct, it is not unlikely, however, that certain actions are expected from lawmakers, stakeholders or the public at large, while not being mandated by law (and thus not subject to the same safeguards, democratic principles or available redress mechanisms). It is, furthermore, unclear how such mechanism impacts the private regulation of tricky cases of information, that may not be illegal but merely unwanted (“lawful but awful”). One could argue that Article 6 DSA in itself strengthens the private actors’ room of

---

66 Section 230(c)(2)(A) of the Communications Decency Act.
69 Cf., e.g., Alphabet (Google) and Meta (Facebook) in public consultation. See also A de Streel et al., Online Platforms’ Moderation of Illegal Content Online: Law, Practices and Options for Reform (Study requested by the European Parliament’s committee on Internal Market and Consumer Protection, 2020), 79 f.
70 See also, e.g., Riis and Schwemer (2019), 11. A Kuczerawy, “The Good Samaritan that wasn’t: voluntary monitoring under the (draft) Digital Services Act” (Verfassungsblog, 12.1.2021) <https://verfassungsblog.de/good-samaritan-dsa/> (last accessed 10 August 2022); on data protection aspects see European Data Protection Supervisor, Opinion 1, 2021 on the Proposal for a Digital Services Act (10 February 2021), 9 ff.
71 On interpretation issues of Art. 6 DSA see, e.g, J Barata, “The Digital Services Act and social media power to regulate speech: obligations, liabilities and safeguards” in IRIS Special, Unravelling the Digital Services Act package (European Audiovisual Observatory, 2021), 12-15.
operation to regulate and may come with the risk of incentivising private actors to – on a voluntary basis – perform general monitoring.71

We may, of course, not forget that private internet intermediaries already today enjoy large discretion and contractual freedom when defining their terms and conditions for the use of their services. In this context, recital 25 DSA further defines the benchmark and specifies that acting in “good faith and in a diligent manner” includes “acting in an objective, non-discriminatory and proportionate manner, with due regard to the rights and legitimate interests of all parties involved, and providing the necessary safeguards against unjustified removal of legal content, in accordance with the objective and requirements of [the DSA].” Considering that algorithmic tools may be used for such purposes, recital 25 DSA notes that such providers should “take reasonable measures to ensure that (…) the technology is sufficiently reliable to limit to the maximum extent possible the rate of errors.” In other words, error rates, i.e. a low percentage of false-positives and false-negatives, seems to be the guiding benchmark for voluntary actions. The DSA, however, remains silent as to what error rate would be acceptable for society.

V. GOING BEYOND THE ECD FRAMEWORK: DUE DILIGENCE OBLIGATIONS

The regulatory novelty of the DSA is that it codifies many of the measures recommended to online platforms by the European Commission in 2018 and in this context puts forward a set of asymmetric due diligence obligations “for a transparent and safe online environment” (Title III) for all internet intermediaries, which should be “clear, effective, predictable and balanced” (recital 34).

Their asymmetric character lies in the fact that the specific obligations are adapted to “type, size and nature” (recital 35) of the concerned intermediary service; in other words, they increase inter alia with the proximity to or influence over content (see Figure 2 below). The most extensive requirements are put upon very-large online platforms (VLOPs), which besides having to comply with the specific rules for VLOPs also fall under the obligations regarding online platforms and internet intermediaries. Transparency reporting obligations, for examples, exist for all providers of intermediary services (Article 13) with additional requirements for online platforms (Article 23) and very large online platforms (Article 33).

| Basic obligations for all providers of intermediary services (Section 1, Arts. 10–13) |
| + Additional obligations for providers of hosting services (Section 2, Arts. 14-15a) |
| + Additional obligations for providers of online platforms (Section 3, Arts. 16-24b) |
| + Provisions applicable to providers of online platforms allowing consumers to conclude distance contracts with traders (Section 3a, Arts. 24c-24e) |
| + Additional obligations for providers of very large online platforms and very large online search engines (Section 5, Arts. 25-33b) |

71 Here, however, an important balancing factor might come into play with the due diligence obligation on terms and conditions in Art. 12(2) DSA, see below.
Figure 2: Structure of due diligence obligations

In the following, instead of providing a full overview, I merely touch upon some of the major themes.

A. THE RELATION BETWEEN DUE DILIGENCE OBLIGATIONS AND THE LIABILITY EXEMPTION FRAMEWORK

The material scope of due diligence obligations connects to the same functional definition that the liability exemptions are based on. An intermediary service according to Article 2(f) DSA is a ‘mere conduit’ service, a ‘caching’ service or a ‘hosting’ service. An online platform is defined in Article 2(h) as a provider of a hosting service “which, at the request of the recipient of the service, stores and disseminates to the public information (...),” unless that activity is only a minor purely ancillary feature. Yet, due diligence obligations introduced in the DSA are separate from the liability exemption framework. In other words, the availability of a conditional liability exemption for an information society service providing ‘mere conduit’, ‘caching’ or hosting is not dependent upon compliance with the horizontal due diligence obligations applicable for said intermediary service. Instead, non-compliance is subject to an enforcement regime and ultimately fines (as briefly mentioned above). Furthermore, according to Article 43a DSA users of a service may seek compensation from providers “against any damage or loss suffered due to an infringement by those providers of their obligations” under the DSA.

The in principle clear-cut distinction, underlined by recital 35 which states that “due diligence obligations are independent from the question of liability of intermediaries which need therefore to be assessed separately”, is somewhat blurred by the fact that Chapter III further specifies certain aspects of the liability exemption framework. This is most notable in relation to hosting, for which notice-and-action procedures are harmonised in the DSA. Article 14(3) DSA, for instance, further refines when a hosting service provider is deemed to have actual knowledge of the illegal information in the sense of Article 5(2) DSA. According to Article 14(3) DSA notices “shall be considered to give rise to actual knowledge or awareness (...),” where they allow a diligent provider of hosting

72 Recital 13 specifies: “Online platforms, such as social networks or online marketplaces, should be defined as providers of hosting services that not only store information provided by the recipients of the service at their request, but that also disseminate that information to the public, again at their request.” Note also the somewhat copyright-linguistically-inspired definition of dissemination to the public concept in Art. 2(i) DSA.


74 Some have argued that such design impacts “individuals’ rights and remedies” and that “linking the obligations in the DSA to the liability exemption may have encouraged the use, development and improvement of automated detection tools of hosting platforms”. M Buiten, “The Digital Services Act: From Intermediary Liability to Platform Regulation” (2021) 12 JIPITEC 361, paras 84–85. Such positive interpretation of available technologies in light of the goal to achieve low error rates, however, seems optimistic. In addition, see also recital 83a and Art. 43a DSA.
services to identify the illegality of the relevant activity or information without a detailed legal examination.”

B. TAMING THE PRIVATE REGULATION OF INTERMEDIARIES

Article 12 DSA concerns the terms and conditions of all intermediary service providers. Whereas the P2B Regulation from 2019 put certain obligations on the terms and conditions of providers of *intermediation* services (Article 3 Regulation (EU) 2019/1150), the terms and conditions of ‘mere conduit’, ‘caching’ and hosting providers have until now not been subject to specific horizontal EU rules. Article 12(1) DSA now obliges service providers to “include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions”. This information requirement includes “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”. Similar to the requirements in the GDPR, it mandates that such terms are written in “clear, plain, intelligible, user friendly and unambiguous language” and in instances where such service is directed at minors to be accompanied by an understandable explanation.

When looking at the room of operation for self-regulation by private internet intermediaries, Article 12(2) DSA is of special interest. It obliges intermediary service providers to “act in a diligent, objective and proportionate manner” and “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” when applying and enforcing their terms and conditions. Undoubtedly, this provision strengthens the fundamental rights balancing, yet its extent (and enforcement) remain vague.”

C. HARMONIZING NOTICE AND ACTION PROCEDURES

The e-Commerce Directive had refrained from harmonising notice-and-action procedures. Article 14 DSA now harmonises notice and action mechanisms and obliges providers of *hosting* services to put in place easy to access and user-friendly mechanisms “to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity

---

75 See also recital 41a DSA. The question of whether and under which conditions a notice should give rise to actual knowledge has been debated, see, e.g. Call for clarification in Standing Committee of the EFTA States, “COMMENT on the Commission Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC - (COM(2020) 825)”, Ref. 21-1935, 29 September 2021, 4; in support, Buiten (2021), 372.

76 Sector-specific for online content sharing service providers, see, e.g., the duty to inform users in terms and conditions of the possibility to upload copyright-protected works falling under a limitation or exception, Art. 17(9) subpara. 4 CDSM Directive.

77 See, however, Article 12(2a) DSA with a further summary requirement for VLOPs and very large search engines.


considered to be illegal content.\textsuperscript{80} It further stipulates in Article 14(2) DSA requirements to ensure “sufficiently precise and adequately substantiated notices”. The provision does not specify a specific timeframe for its decision as demanded by some voices during the legislative process. Instead, Article 14(6) DSA requires to take decisions “in a timely, diligent, non-arbitrary and objective manner”. Since such actions likely often are partly or fully automised, Article 14(6) in connection with Article 14(5) requires that users are informed of that automation.

As further novelty, Article 15 DSA introduces an explanation requirement towards affected users in form of a statement of reasons. Such “clear and specific statement of reasons” must be provided in instances where the visibility of the content is restricted by removal, disabling or demotion (lit. a), demonetisation (lit. b), suspension of the service (lit. c) or suspension of the user’s account (lit. d). Article 15(2) DSA contains a catalogue of minimum information provided in such statement including the extent of the decision, “facts and circumstances relied on in taking the decision” as well as “clear and user-friendly information on the redress possibilities”.

In the context of online platforms, Articles 17 and 18 DSA set forth a detailed internal complaint mechanism as well as an out-of-court dispute settlement process. Such “effective” internal complaint handling-system must be provided by the online platform according to Article 17(1) DSA to users of the service, “including individuals or entities that have submitted a notice”. The handling of such complaint in turn must in accordance with Article 17(3) DSA be performed in a “timely, non-discriminatory, diligent and non-arbitrary manner” and following a successful complaint the decision must be reversed without undue delay. Importantly, however, such decision may not be taken “solely on the basis of automated means” meaning that while the original decision may be fully automised, the complaint about it may not. Instead, it must be taken “under the control of appropriately qualified staff”.\textsuperscript{81}

Another aspect, related to notice and action mechanisms, relates to “trusted flaggers” and measures against misuse. Article 19 DSA codifies parts of Recommendation 2018 and obliges online platforms to take “necessary technical and organisational measures to ensure that notices submitted by trusted flaggers, acting within their designated area of expertise” are treated with priority and undue delay.\textsuperscript{82} It also sets forth an accountability mechanism, e.g., by requiring transparency report. Since (voluntary) trusted flagger arrangements also exist outside the platform-reality (e.g., domain name registries), it is, however, surprising that the lawmaker refrained from introducing such safeguards for all intermediary services.\textsuperscript{83} Similarly, Article 20 DSA only applies to online platforms. According to Article 20(2) DSA, the frequent submission of “manifestly unfounded notices or complaints” shall lead to suspension of the processing of notices and complaints “for a reasonable period of time”. Furthermore, according to Article 20(1) DSA users that frequently provide “manifestly illegal content” shall be suspended “for a reasonable period of time and after having issued a prior warning”.

\textsuperscript{80} The EFTA Standing Committee, for example, criticized that the Commission’s proposal “does not include explicit safeguards against over-removals of certain types of content” pointing \textit{inter alia} to the moderation of content made available by editorial media, see Standing Committee of the EFTA States, “EEA EFTA COMMENT on the Commission Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC - (COM(2020) 835)”, Ref. 21-1995, 29 September 2021, 4.

\textsuperscript{81} Recital 44 DSA adds that the complaint is subject to human review where automated means are used.


\textsuperscript{83} See in this vein the recommendation by Schwemer, Mahler and Styri (2021), 29.
D. ONE INSTRUMENT TO SOLVE ALL ISSUES?

Whereas the above aspects fall into a broad updating of the e-Commerce Directive, the DSA has also been the instrument of choice by the European Parliament and the Council to address a multitude of concurrent platform-related issues (some which could have also been “home” in other legislative fora). It addresses, for example, issues related to advertising (e.g., Article 24 regarding Advertising on Platforms as well as the additional online advertising transparency rules for VLOPs in Article 30 DSA) that could also have been addressed in the arena of the ePrivacy Directive or a GDPR trajectory. Article 23a DSA addresses dark patterns of online platforms and stipulates that they shall not design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of recipients of their service to make free and informed decisions. Article 24b concerns the online protection of minors. Besides the moderation of illegal information, also the algorithmic recommendation of content has become a central issue online platforms. In this context, Article 24a DSA introduces a transparency obligation on online platforms. In addition to this, very large online platforms according to Article 29 DSA are also obliged to provide “at least one option for each of their recommender systems which is not based on profiling”.

Thematically also online marketplaces, which were considered a separate issue by the European Commission, featured prominent in Parliament and Council discussions as well as the final text. Most significantly, however, in Section 4 on Additional obligations for providers of very large online platforms and very large online search engines, Articles 26 and 27 DSA put in place a risk assessment and risk mitigation mechanism for VLOPs. Furthermore, Article 27a DSA introduces a crisis response mechanism. A detailed analysis is outside the scope of this chapter.

E. OVERLAPS: THE RELATION BETWEEN THE DSA AND OTHER LEGAL FRAMEWORKS

---

84. The Commission’s proposal had only addressed VLOP, see criticism in SF Schwemer, “Recommender Systems in the EU: From Responsibility to Regulation” (2022) 1 Morals & Machines 60–69 <https://doi.org/10.5771/2747-5174-2021-2-60>.


86. Pushed especially by Denmark, see, e.g., Schaldemose report and Statement by Denmark, in Council of the European Union, Note from General Secretariat of the Council to Council, 13203/21 ADD 1 , Brussels, 18 November 2021.

87. Note the extension effect in Art. 33a DSA, whereby the majority of VLOP provisions also is applicable to very large online search engines.

88. Namely risks relating to “the dissemination of illegal content through their services”, “any actual or foreseeable negative effects for the exercise of fundamental rights (…)”, “any actual or foreseeable negative effects on civic discourse and electoral processes, and public security”, or “any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health, minors and serious negative consequences to the person’s physical and mental well-being”, cf. Art. 26(1) lit. (a)-(ca) DSA.

89. See also recital 59a DSA.

90. On the proposal, see, e.g., G Spindler, „Der Vorschlag für ein neues Haftungsregime für Internetprovider – der EU-Digital Services Act, Teil 2: Große und besonders große Plattformen“ [2021] Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 653 (in German)
Given the broad scope of the DSA and the high topicality of many of its regulatory themes, an important question regards the interplay between the DSA and other legal frameworks; be it existing or future sector-specific regulation, other horizontal frameworks or national legislation. How do different frameworks interact? What room is left, for example, for national rules to complement the DSA? Even before the official proposal of the DSA, for example, the Commission asked France to pause its legislative efforts to regulate hate speech with a view to await the Commission’s draft proposal. Also a more recent attempt to horizontally regulate “social media platforms” in Denmark from March 2022 was blocked by the European Commission.

The DSA recalls that “diverging national laws negatively affect the internal market” (recital 2), which is one of the reasons for the choice of instrument. Recital 9 DSA now underlines the full harmonisation approach and specifies as starting point that “Member States should not adopt or maintain additional national requirements on the matters falling within the scope” of the DSA. Article 1a (4) DSA and the comprehensive recital 10 clarify that the DSA is without prejudice to other Union law regulating related matters, such as the AVMSD or the GDPR. The relation to copyright has a devoted recital 11 stating that CDSM Directive “which establish specific rules and procedures that should remain unaffected” and manifests its sector-specific carve-out character. There remain, however, many questions regarding the (product-safety inspired) proposal for an Artificial Intelligence Act have been separate from similar discussions in the DSA, notably in relation to recommender systems and algorithmic content moderation and has not found its way into the provision clarifying overlaps.

---

91 Note that the interplay with other legal acts is also underlined as special area of interest in the Commission’s evaluation of the DSA, cf. recital 102.
96 Buiten (2021), 371, for example argues that the Good Samaritan clause also applies when actions taken to comply with Art. 17 CDSMD, whereas Quintais and Schwemer (2022) argue that there would be little need of and room for the application of Art. 6 DSA.
In the future, in any case, internet law scholars, practitioners and courts alike will likely have to engage more with these questions.

VI. CONCLUSION

For some time, opening the e-Commerce Directive’s liability exemption framework was perceived as potentially opening Pandora’s box. Instead, the Digital Services Act represents a GDPR-like moment for internet law in the EU and beyond. Much of the intermediary liability exemption regime that we know from the e-Commerce Directive remains intact and is updated. Yet, there are notable adjustments including the Good Samaritan clause as well as further specifications of the notice-and-action mechanisms in the due diligence obligations of the DSA. Even though many major developments are concerning due diligence obligations of (very large) online platforms, we may not overlook that the DSA is a regime governing more technical internet intermediaries, too.

The e-Commerce Directive, despite many issues (including the centralization of a few very large online platforms, the scale of information and the role of automation in handling it) that the original drafters had not foreseen in the late 1990s, has served relatively well for more than two decades through fast-paced developments.

It remains to be seen whether the DSA’s regulatory design will allow this Regulation to be similarly future proof. The European legislator opted for focusing on the most pressing issues of today which relate to (very) large online platforms and their power over (illegal and legal) information in our modern digital democracies. This may have been to the detriment of a more use case- and technology neutral framework that also accounts for future technological and business developments that influence the way we use the “internet”. Instead of overloading one Regulation with the task to of regulating the very (relatively technology-neutral) principles of how intermediaries act and the task of solving very specific pressing issues, another design could have been a framework Regulation that is accompanied by smaller, specific, and more granular acts addressing issues such as advertising or similar. Such design might have made future revisions and interventions politically less cumbersome. Such revisions might become necessary; the DSA represents a “realistic” approach to regulating the unfathomable amount of information on the internet by both encouraging and taming the (algorithmic) power of private actors. Whether a right balance that can last for another two decades is struck and to what extent the DSA is able to capture coming fast-paced developments and new services, remains to be seen.

99 See also the evaluation mechanism contained in Art. 73 DSA.