A New Order: The Digital Services Act and Consumer Protection

Caroline CAUFFMAN* and Catalina GOANTA**

On 16 December 2020, the European Commission delivered on the plans proposed in the European Digital Strategy by publishing two proposals related to the governance of digital services in the European Union: the Digital Services Act (DSA) and the Digital Markets Act (DMA). The much-awaited regulatory reform is often mentioned in the context of content moderation and freedom of expression, market power and competition. It is, however, important to bear in mind the contractual nature of the relationship between users and platforms and the additional contracts concluded on the platform between the users, in particular traders and consumers. Moreover, the monetisation offered by digital platforms has led to new dynamics and economic interests. This paper explores the reform proposed by the European Commission by means of the DSA by touching upon four main themes that will be addressed from the perspective of consumer protection: (1) the internal coherence of European Union law; (2) intermediary liability; (3) the outsourcing of solutions to private parties; and (4) digital enforcement.

I. Introduction

On 16 December 2020, the European Commission delivered on the plans proposed in the European Digital Strategy, "Shaping Europe's Digital Future",[1] by publishing two proposals related to the governance of digital services in the European Union (EU). The Digital Services Act package includes two regulation proposals: the Digital Services Act (DSA) and the Digital Markets Act (DMA). According to the European Commission, these legislative proposals have two goals: (1) promoting fundamental rights in digital services; and (2) promoting technological innovation through the establishment of common rules for digital service providers in the European Single Market and beyond.[2]

* Maastricht University, Bouillonstraat 1–3, 6211 LH Maastricht, The Netherlands; email: caroline.cauffman@maastrichtuniversity.nl.

** Maastricht University, Bouillonstraat 1–3, 6211 LH Maastricht, The Netherlands; email: catalina.goanta@maastrichtuniversity.nl.

1 European Commission, "Shaping Europe's Digital Future" (*European Commission*, February 2020) <https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf>.

2 European Commission, "Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act)" COM(2020) 825 final (European Commission, December 2020), p 2 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en>.

European Journal of Risk Regulation, 12 (2021), pp. 758–774 doi:10.1017/err.2021.8

The Commission's plans for reshaping European rules on platform governance have raised high expectations from a plethora of stakeholders.[3] While the interests involved may be difficult to align, the general opinion on whether this legislative reform is fit to tackle the complexity of the digital economy at the European and global level is sharply divided: some stakeholders expected the reform to be more daring, while others find that it imposes too harsh obligations.[4] Such divergence in reactions is an accurate reflection of the tension between the need to further expand the coverage of fundamental rights into the private spheres of Big Tech infrastructures and the need for regulatory subsidies to nurture competition, innovation and economic development.

The much-awaited regulatory reform is often mentioned in the context of content moderation and freedom of expression, market power and competition. It is, however, important to bear in mind the contractual nature of the relationship between users and platforms and the additional contracts concluded on the platform between the users, in particular those between traders and consumers. Moreover, the monetisation offered by digital platforms has led to new dynamics and economic interests, leaving platforms with the role of intermediaries in the supply of digital content, such as media content. Particularly in this industry, content monetisation has been raising new questions about the fitness of existing regulation.[5]

This contribution explores the reform proposed by the European Commission by means of the DSA. The DSA is structured as follows: Chapter I establishes its scope and defines the key concepts used. Chapter II covers the liability of providers of intermediary services, building on earlier standards set by the e-Commerce Directive.[6] Chapter III sets out due diligence obligations for a transparent and safe online environment, distinguishing between providers of intermediary services in general, online platforms and very large online platforms. Chapter IV deals with the DSA's implementation and national and supranational cooperation, as well as sanctions and enforcement, by setting out new public administration bodies such as the Digital Services Coordinators.

The DSA is a long and complex proposal that is likely to give rise to extensive discussions in academia and in the European Parliament. This contribution concentrates on four main themes, addressed from the perspective of consumer protection: (1) the internal coherence of EU law; (2) intermediary liability; (3) the outsourcing of solutions to private parties; and (4) digital enforcement.

[3] S Schechner, "Tech Giants Face New Rules in Europe, Backed by Huge Fines" (*The Wall Street Journal*, 16 December 2020) <https://www.wsj.com/articles/tech-giants-face-new-rules-in-europe-backed-by-huge-fines-11608046500>.

[4] L Kayali and T Larger, "5 challenges to the new EU digital rulebook" (*Politico*, 16 December 2020) <https://www.politico.eu/article/5-challenges-to-the-new-eu-digital-rulebook/>.

[5] C Goanta and S Ranchordás, *The Regulation of Social Media Influencers* (Cheltenham, Edward Elgar 2020); R Caplan and T Gillespie, "Tiered governance and demonetization: the shifting terms of labor and compensation in the platform economy" (2020) 6(2) Social Media & Society 1.

[6] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (e-Commerce Directive) [2000] OJ L 178. See also European Commission, supra, note 2, at 1.

II. The internal coherence of EU law

The DSA proposal aims to update existing rules on platform responsibilities in the provision of digital services by means of revising the legal regime enacted by Directive 2000/31/EC (the e-Commerce Directive). In doing so, the Commission's Inception Impact Assessment reveals the alignment of this regulatory exercise with the "Better Regulation" agenda launched back in 2015.[7] The "Better Regulation" agenda focused on more transparency and consultation in law-making, as well as on using more evidence-based approaches to understanding the impact of proposed legislation.[8] European regulatory reforms need to be consistent with other EU policies and legal frameworks, as acknowledged in the DSA Explanatory Memorandum.[9] In justifying the cross-sectoral scope of the DSA, the Memorandum indicates that sector-specific instruments are limited both procedurally, as they do not sufficiently incorporate procedures for dealing with illegal content, and substantively, as they are either focused on narrow issues (eg copyright, child abuse material, illegal hate speech, etc.) or on specific platforms (eg audiovisual sharing platforms).[10] The DSA is based on a horizontal approach that is complementary to a series of existing EU legislative instruments that it would leave unaffected and with which it would be consistent,[11] such as Directive (EU) 2018/1808 (Audiovisual Media Services Directive)[12] or Directive (EU) 2019/2161 (Omnibus Directive).[13] Upon a closer look at the body of rules in the proposed DSA, however, a different picture emerges, which can be explored both conceptually and practically.

First of all, considering the conceptual systematisation of European law, the coherence issues posed by European harmonisation rules and policies are by no means new.[14] As a result of the principles of conferral, subsidiarity and proportionality on which the EU's competences are based (Article 5 TEU),[15] EU legislative action has been mostly sectoral, focused on partial legal harmonisation (eg maximum harmonisation directives, regulations) and responding to specific market developments (eg technological developments). While the DSA Explanatory Memorandum acknowledges the

[7] Eg see A Alemanno, "How much better is better regulation? Assessing the impact of the Better Regulation Package on the European Union – a research agenda" (2015) 6(3) European Journal of Risk Regulation 344; U Pachl, "Repercussions of the European Commission's Better Regulation Agenda on consumer interests and policy" (2015) 6(3) European Journal of Risk Regulation 375.

[8] European Commission, "Better Regulation Agenda: enhancing transparency and scrutiny for better EU law-making" (*European Commission*, 19 May 2015) <https://ec.europa.eu/commission/presscorner/detail/en/IP_15_4988>.

[9] European Commission, supra, note 2, at 4.

[10] ibid.

[11] European Commission, supra, note 2, at 8.

[12] Directive (EU) 2018/1808 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) [2018] OJ L 303.

[13] Directive (EU) 2019/2161 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (Omnibus Directive) [2019] OJ L 328.

[14] Eg see J Smits, "Full harmonization of consumer law? A critique of the draft directive on consumer rights" (2010) 18 European Review of Private Law 5.

[15] See S Garben and I Govaere (eds.), *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future* (Oxford, Hart Publishing 2017).

drawbacks of the lack of systematisation of existing EU legislation, it does not fundamentally improve this. Instruments such as Directive 93/13/EEC (Unfair Contract Terms Directive; UCTD),[16] Directive 2005/29/EC (Unfair Commercial Practices Directive; UCPD)[17] or Regulation (EU) No 524/2013 (Online Dispute Resolution (ODR) Regulation)[18] equally contain cross-sectoral and/or procedural rules that remain fully applicable to unlawful content. These examples are only a few illustrations of a wider array of rules that make up a body of content regulation from the perspective of consumer protection.

This takes us to the second point, namely that of the practical implications of the lack of coherence in European law, emphasised by the DSA rules. An illustration of such practical implications can be seen in Article 22 DSA, dealing with the traceability of traders. Found in Section 3 of the DSA, which does not apply to micro or small enterprises, Article 22 imposes an obligation on platforms intermediating online contracts between traders and consumers to obtain identifying information from traders.[19] In addition to this, platforms also need to make "reasonable efforts" to verify the reliability of the information submitted. In general, platforms are not required to disclose this information to their users (eg consumers or other traders). However, Articles 22(5) and 9 indicate how the obtained information must be made available to national authorities under the procedural frameworks specified in these articles.

Pursuing the transparency of service providers is not a new policy goal. Articles 5 and 6 of the e-Commerce Directive had established obligations for service providers to disclose information about themselves to consumers and public authorities. Similarly, the Consumer Rights Directive (CRD) already requires online traders to disclose a wide array of information to consumers before the conclusion of a contract. In addition, the Omnibus Directive introduced Article 6a in the CRD, dealing specifically with the information duties of platforms vis-à-vis consumers who engage in contracts with third parties using the platform architecture.

When comparing these approaches to transparency, the DSA's duty to investigate stands out from earlier requirements in three ways. First is the platform's obligation to retrieve information from traders. The e-Commerce Directive and the CRD impose obligations on traders themselves to disclose this information to consumers. Second, the DSA specifies that platforms are under an obligation to take reasonable steps to verify this information, which is not part of the disclosures under the e-Commerce Directive and the CRD. Lastly, the DSA does not impose a duty of disclosure on

[16] Council Directive 93/13/EEC on unfair terms in consumer contracts (Unfair Contract Terms Directive) [1993] OJ L 95.

[17] Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC and Regulation (EC) No 2006/2004 (Unfair Commercial Practices Directive) [2005] OJ L 149.

[18] Regulation (EU) No 524/2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (ODR Regulation) [2013] OJ L 165.

[19] According to Art 22, this information, also referred to as "know your customer", includes the trader's name, address, telephone and email address, a copy of their identification document or any other electronic identification, their bank account details (for natural persons), the trade register in which they registered and their registration number or equivalent means of identification in that register (if they are registered in such a register and "a self-certification by the trader committing to only offer products or services that comply with the applicable rules of Union law".

platforms after the information has been obtained, unless this information is requested by public authorities in relevant procedural processes.

Although the DSA's "know your business customer" approach may differ from the transparency rules enshrined in earlier legislation in the three ways mentioned above, it can be argued that inconsistencies with consumer instruments such as the CRD and the UCPD still remain.

The CRD is an instrument that focuses on the direct relationship between traders and consumers inter alia in the context of e-commerce, where intermediation has generally been performed by online marketplaces.[20] The DSA focuses on the responsibility of platforms as intermediaries. As an illustration, according to the CRD, it is up to traders using the Amazon marketplace to make the consumer disclosures embedded in the CRD. Amazon itself ought to make consumer disclosures to the extent that it sells goods or provides services directly to consumers. However, as an intermediary, Amazon offers platform functionalities (also known as platform affordances)[21] that traders use to make their disclosures (eg the visual space on the marketplace website where traders can share their contact details and withdrawal rights information). What is more, consumer trade is no longer limited to online marketplaces within its original meaning, as social media platforms have introduced their own complete marketplaces (eg Facebook), developed functionalities that facilitate the sale of goods or the provision of services (eg Instagram's business accounts) or integrated new types of transactions between consumers and potential traders (eg Twitch's token system).[22] Based on Article 6a CRD as amended by the Omnibus Directive, online marketplaces already need to inform consumers as to whether the third party offering goods, services or digital content is a trader or not, based on the declaration made to them by the third party and as to how obligations related to the contract are shared between third parties offering the goods, services or digital content and providers of online marketplaces.[23] Moreover, given that mandatory consumer disclosures by traders may be limited in some ways by platform functionalities, an argument can be made that platforms already have disclosure duties (at least duties to enable traders using their platform to fulfil their disclosure duties) according to the CRD, even as intermediaries and not as traders interacting directly with consumers. As far as the UCPD is concerned, new obligations integrated by the Omnibus Directive touch upon the relationship between platforms, traders and consumers, to the extent that not disclosing the identity of the trader may lead to an unfair commercial practice. More specifically, Article 7(4)(f) UCPD considers as material the information regarding whether a third party making goods or services available on a marketplace is a trader or not. The omission of material information is a part of the test enshrined in Article 7 for misleading omissions, which represent a particular category of unfair commercial practices.

[20] The CRD is equally applicable to web shops where traders offer goods or services directly to consumers.

[21] J Hemsley, J Jacobson, A Gruzd and P Mai, "Social media for social good or evil: an introduction" (2018) 4(3) Social Media + Society 1.

[22] Facebook Marketplace (*Facebook*, 17 January 2021) <https://www.facebook.com/marketplace>; Instagram Business (*Instagram*, 17 January 2021) <https://business.instagram.com/getting-started>; Twitch, "iOS Sub Tokens Guide" (*Twitch*, 17 January 2021) <https://help.twitch.tv/s/article/ios-sub-tokens?language=en_US>.

[23] See also Recital 27, Omnibus Directive.

What the CRD and the consolidated version of the UCPD show is that the EU *consumer acquis* already has employed a lot of mandatory disclosures. These disclosures have traditionally been established between traders and consumers as a means to offer more transparency to the digital trading ecosystem. The DSA tackles transparency in a different manner, which ought to be, in principle, complementary to what the consumer acquis provides for. However, in practice, it is questionable how cohesive these approaches really are. From the trader's perspective, information needs to be provided to platforms (non-public) and consumers (public). From the consumer's perspective, they will be given information about traders on the marketplaces and websites operated by said traders, and perhaps (but not necessarily) on other platforms (eg social media). From the platform's perspective, there may be disclosure obligations owed to consumers in the case of offering goods or services directly, but also when merely intermediating these offers, as well as the duty to investigate, verify and share this information with public authorities.

All in all, while the policy objective is clear (platforms need to collect information on traders using their platform and to make reasonable efforts to check this information in order to offer a certain level of protection to their users on the buyer side), what is unclear is how this new duty to investigate and verify trader information will fare with existing mandatory disclosures already borne by traders. Moreover, the DSA's approach seems to be detached from long-standing practices employed by some platforms in terms of verification programmes. For instance, Airbnb's verification system entails that the host needs to submit a national ID,[24] but other platforms use such systems to confirm the identity of public figures, celebrities and brands. Verification programmes are equally used by social media platforms and marketplaces to diminish fraud.[25] What is interesting about this type of platform functionality is that, on the one hand, it reflects an internal verification process that allows the platform to ask for certain documentation in order to certify a user's identity. On the other hand, this certification has a public dimension (eg a check sign or a badge) that is shared with consumers and acts as a trust mark. The resulting process combines the platform's current self-imposed duty to investigate with a voluntary disclosure, all to improve consumer trust in the platform environment.

III. Intermediary liability

While the DSA deletes Articles 12–15 of the e-Commerce Directive with regard to the liability of intermediary service providers, the rules it introduces instead (Articles 3–9) do not change much. They maintain the rules from the e-Commerce Directive, and in addition, they mainly codify the interpretation that the Court of Justice has given of these rules.[26]

[24] Airbnb, "How does it work when Airbnb verifies your identity?" (*Airbnb*, 17 January 2021) <https://www.airbnb.com/help/article/1237/how-does-it-work-when-airbnb-verifies-your-identity>.

[25] Instagram, "Verify Your Business on Instagram" (*Instagram*, 17 January 2021) <https://help.instagram.com/369148866843923>.

[26] See also European Commission, supra, note 2, at 3.

Similarly to the e-Commerce Directive, the DSA distinguishes between intermediary service providers providing mere conduit, caching and hosting services. In this section, we will focus on the liability of online platforms. Under the DSA, online platforms are a subcategory of hosting providers, which are themselves a subcategory of intermediary service providers.[27] It follows that, in general, online intermediary platforms benefit from the liability exemption contained in Article 5(1) DSA, corresponding with the so-called "hosting exemption" under the e-Commerce Directive. Except when the DSA provides otherwise, online platforms will

> not be liable for the information stored at the request of a recipient of the service on condition that the provider:
>
> (a) does not have actual knowledge of the illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or
>
> (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.[28]

However, pursuant to Recital 6 DSA, providers of intermediary services constituting an integral part of another service (eg transportation, accommodation or delivery services) "which is not an intermediary service as specified in the case law of the Court of Justice of the European Union" fall outside the scope of the DSA and consequently cannot benefit from the exemption. Providers of services of the Uber type therefore cannot benefit from the exemption.[29] Even though Recital 6 DSA mentions accommodation services, it is to be noted that the Court of Justice held that the intermediary service in the business model of Airbnb did not constitute an integral part of the accommodation services, so that the exemption will remain available.[30]

Furthermore, pursuant to Recital 18, first sentence, of the DSA, the exemption does 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.

This clearly refers to the neutrality requirement that the Court of Justice introduced in the cases *Google France/Louis Vuitton* and *L'Oréal/eBay*.[31] It is not entirely clear, however, whether the neutrality requirement is intended to remain applicable in exactly the same way under the DSA as it was understood in the case law of the Court of Justice. According

[27] Art 2(h) and Recital 13 DSA.

[28] Art 5(1) DSA.

[29] C-434/15 *Asociación Profesional Elite Taxi* [2017] EU:C:2017:981; C-320/16 *Uber France* [2018] EU:C:2018:221.

[30] C-390/18 *Airbnb Ireland* [2019] ECLI:EU:C:2019:1112.

[31] C-236/08 *Google France SARL and Google Inc* [2010] ECLI:EU:C:2010:159; C&x2011;324/09 *L'Oréal* [2011], ECLI:EU:C:2011:474.

to the Court of Justice, the neutrality requirement is not met when the intermediate service provider "has provided assistance which entails, in particular, optimizing the presentation of the offers for sale in question or promoting those offers".[32] Yet, the second sentence of Recital 18 only mentions that the exemption 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", which can be used to plead for a much narrower interpretation.

In any case, providers of intermediary services no longer need to fear that the neutrality requirement would make them lose the benefit of the liability exemption when carrying out "voluntary own initiative investigations or other activities aimed at detecting, identifying and removing, or disabling of access to, illegal content" (Article 6).

While the DSA removes the risks for intermediary service providers to carry out voluntary monitoring of the activities on their platforms, it confirms the prohibition for the Member States to impose on such service providers a general monitoring or active obligation to seek facts or circumstances indicating illegal activity, as contained in the e-Commerce Directive (Article 7 DSA). However, like the e-Commerce Directive, the proposal does not withhold courts or administrative authorities, in accordance with Member States' legal systems, of requiring an intermediary service provider to terminate or prevent a specific infringement (Article 5(4)). As opposed to the e-Commerce Directive, the proposal further elaborates and harmonises the conditions to be met by such orders. They need to contain a statement of reasons explaining why the information is illegal content, by reference to the specific legal provision infringed, one or more exact uniform resource locators and, where necessary, additional information enabling the identification of the illegal content concerned and information about redress available to the provider of the service and to the recipient of the service who provided the content. Moreover, the order's territorial scope must not exceed what is strictly necessary to achieve its objective and the order is to be drafted in the language declared by the provider and to be sent to the point of contact, appointed by the provider (Article 8).

The e-Commerce Directive left it to the Member States to determine the conditions for imposing obligations on intermediary service providers (in fact, information service providers) to inform the competent authorities of illegal information provided or illegal activities undertaken by the recipients of their services or of information enabling the identification of such recipients.[33] By contrast, the DSA contains in Article 9 detailed, harmonised rules on this point. Unfortunately, these rules restrict the powers of national authorities. The information to be provided must be "a specific item of information about one or more specific individual recipients of the service", and the order must contain

> a statement of reasons explaining the objective for which the information is required and why the requirement to provide the information is necessary and proportionate

[32] *L'Oréal*, para 116. See also *Google France SARL and Google Inc*, para 120.

[33] Art 15(2) e-Commerce Directive.

> to determine compliance by the recipients of the intermediary services with applicable Union or national rules, unless such a statement cannot be provided for reasons related to the prevention, investigation, detection and prosecution of criminal offences,

as well as "information about redress available to the provider and to the recipients of the service concerned". Moreover, the order should only require the intermediary service provider to provide information already collected for the purposes of providing the service and that lies within its control, and the order is to be drafted in the language declared by the provider and sent to the point of contact appointed by that provider (Article 9).

Even more fundamental is that the DSA only contains Union-wide rules on intermediary service providers' *exemption* from liability, and no Union-wide provisions on the conditions under which intermediary service providers incur liability.[34] The conditions under which they incur liability are determined by other rules of EU or national law. Leaving the determination of the conditions for liability of intermediaries to the Member States will limit the capacity of the DSA to create a level playing field throughout the EU. However, a minimum level of protection for intermediary service providers is guaranteed by the fact that EU rules prevail over national rules, so that the national laws of the Member States may not affect the exemption from liability contained in the DSA.

While the Explanatory Memorandum mentions that the liability exemptions as contained in the e-Commerce Directive received wide support from the stakeholders, it cannot be denied that this exemption has also been subject to criticism. For example, it has been argued that, in the case of online marketplaces, consumers often rely on the brand image of the platform and even consider the platform as their contracting party rather than the party who uses the platform to commercialise its goods and services.[35] The DSA tries to address this criticism by providing in Article 5(3) that the exemption does

> *not* apply with respect to liability under consumer protection law of online platforms allowing consumers to conclude distance contracts with traders, where such an online platform *presents the specific item of information or otherwise enables the specific transaction at issue in a way that would lead an average and reasonably well-informed consumer* to 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*.[36]

[34] Recital 17 DSA.

[35] Note that the Omnibus Directive already tried to solve this problem by introducing Art 6a CRD requiring online marketplaces in essence to inform consumers on whether the third party offering the goods, services or digital content is a trader or not and the legal consequences thereof, as well as, where applicable, how the obligations related to the contract are shared between the third party offering the goods, services or digital content and the provider of the online marketplace. See also Art 7(4) f UCPD, equally introduced by the Omnibus Directive.

[36] Art 5(3) DSA, emphasis added.

The question arises, however, as to whether this offers consumers sufficient protection. Although the criterion of the "average and reasonably well-informed consumer" found in Article 5(3) DSA is widely used in consumer law, its interpretation and application give rise to a certain level of legal uncertainty[37] and open the door to discussions in legal proceedings where the platform is likely to benefit from representation by high-quality lawyers, while the consumer may often even choose to represent itself to save costs.[38] In addition, the expression "under its authority or control" is likely to give rise to legal uncertainty and discussions in legal proceedings.

Moreover, Article 5(3) DSA does not solve the problem that platforms offer sellers and service providers the opportunity to easily reach out to a large number of consumers using the professional outlook of the platform, even when they lack the financial means or willingness to compensate harm caused to consumers.[39] Similarly, intermediaries that facilitate content sharing create an environment that can be abused to anonymously post information that is harmful to others. A typical example of such abusive conduct is known as doxing: posting personal information of individuals who, for example, made a contested statement, in view of inciting opponents to physically harass them.[40] In either case, the intermediary creates an environment that facilitates third parties to cause harm to others. When the intermediary acts with the intention to make profits and the harmed party is an individual, this seems to justify a liability regime where the intermediary is liable towards the individual for the harm caused and can afterwards exercise the victim's right of redress against the infringer.[41] This is all the more the case since the intermediary will generally be in a better position to bear the costs of litigation.[42] All in all, the DSA appears to be more concerned with providing legal protection and certainty to intermediary service providers than to consumers using their services.

IV. Outsourcing solutions to private entities

The DSA foresees an important role for private entities both when it comes to the further elaboration of the regulatory framework applicable to intermediary service providers and to its enforcement. For example, it provides that the Commission shall support and promote the development and implementation of voluntary industry standards set by

[37] On the different interpretations, see K Purnhagen, "More reality in the CJEU's interpretation of the average consumer benchmark – also more behavioural science in unfair commercial practices?" (2017) 8(2) European Journal of Risk Regulation 437–40.

[38] Moreover, it is noteworthy that the proposal does not contain an exemption for vulnerable consumers similar to Art 5(3) UCPD.

[39] In our opinion, the duty Art 22 imposes upon the platform to request certain information from traders and to make reasonable efforts to assess the reliability of certain elements thereof does not offer sufficient protection either.

[40] On this practice in the USA, see N Homchick, "Reaching through the ghost doxer: an argument for imposing secondary liability on online intermediaries" (2019) 76(3) Washington and Lee Law Review 1307, 1327–28.

[41] See also M Buiten, A de Streel and M Peitz, "Rethinking liability rules for online hosting platforms" (2020) 28(2) International Journal of Law and Information Technology 149.

[42] ibid, at 155. See also SG Sartor, "Providers liability: From the eCommerce Directive to the future" (*European Parliament*, October 2017) p 10 <https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf>.

relevant European and international standardisation bodies on a number of technical matters, such as electronic submission of notices by trusted flaggers (Article 34). In addition, it provides that the Commission and the European Board for Digital Services (see further in Section V) shall encourage and facilitate the drawing up of codes of conduct at the Union level to contribute to the proper application of the Regulation, particularly on competition and the protection of personal data (Article 35) and on online advertising (Article 36). In addition, the Commission shall, as the case may be, encourage and facilitate the drawing up of crisis protocols for addressing crisis situations strictly limited to extraordinary circumstances affecting public security or public health (Article 37).

Although the DSA reserves a certain governmental intervention in the drawing up of these documents as well as the analysis of their performance, the Recitals stress their voluntary character. The role of the Commission is repeatedly described in weak terms: "facilitate", "invite", "aim to ensure".[43] It is noteworthy that the involvement of civil society organisations is only mentioned with regard to codes of conduct dealing with cases where systemic risks arise, online advertising codes and crisis protocols.[44]

The outsourcing of rule-making to private parties (albeit within the boundaries of the applicable mandatory law) is a global tendency.[45] Nevertheless, this "privatisation" of Internet governance is subject to heavy criticism from a fundamental rights perspective.[46] From the perspective of the legitimacy of rule-setting, a distinction can be made between input legitimacy and output legitimacy.[47] Input legitimacy refers to the representative character of the rule-making process and requires that "all citizens' interests are sufficiently taken on board and protected".[48]

Output legitimacy refers to the outcome of a rule-setting process. Rules are considered legitimate from an output legitimacy perspective if they manage to reach the desired result.[49] The latter can only be assessed once the rules have been determined. In the past, however, attempts at self-regulation in the field of Internet governance have been ineffective.[50]

In addition, when it comes to ensuring compliance with both EU and national laws and self-regulatory norms, private parties have a role to play under the DSA. As mentioned in

[43] Where standards are developed by European standardisation organisations, a certain involvement of civil organisations is guaranteed as well.

[44] Arts 35(2), 36(1) and 37(3) DSA.

[45] GF Frosio, "Reforming intermediary liability in the platform economy: a European digital single market strategy" (2017) 112 Northwestern University Law Review 19.

[46] Eg see ibid, at 19–46; GF Frosio "Why keep a dog and bark yourself? From intermediary liability to responsibility" (2018) 26(1) International Journal of Law and Information Technology 1–33.

[47] F Scharpf, *Governing in Europe: Effective and Democratic?* (Oxford, Oxford University Press 1999).

[48] L Senden, "Towards a more holistic legitimacy approach to technical standardisation in the EU" in M Eliantonio and C Cauffman (eds.), *The Legitimacy of Standardisation as a Regulatory Technique: A Cross-Disciplinary and Multi-Level Analysis* (Cheltenham, Edward Elgar 2020) p 27.

[49] C Harlow, "Accountability as a value in global governance and for global administrative law", in G Anthony, J-B Auby, J Morison and T Zwart (eds.), *Values in Global Administrative Law* (Oxford, Hart Publishing 2011) p 182.

[50] BEUC, "Making the digital services act work for consumers. BEUC's recommendations" (*BEUC*, 2020) <https://www.beuc.eu/publications/beuc-x-2020-031_making_the_digital_services_act_work_for_consumers_-_beucs_recommendations.pdf>.

Section III, the Proposal does not impose a general monitoring obligation on intermediary service providers, but it removes an obstacle to such voluntary monitoring by providing that it will not lead to the loss of the liability exemption contained in Article 6.

As such, the DSA does not oblige but allows the intermediaries themselves to carry out voluntary monitoring on a general basis, in addition to their duty to make sure that injunctions given by the competent authorities are complied with by removing and preventing the reappearance of illegal information.

Voluntary monitoring by intermediaries as a means to protect users against illegal goods and information sounds good. However, on further consideration, things are more complicated. A first problem is related to the definition of the concept "dissemination of information to the public" that is an essential component of the definition of an online platform. The DSA defines the latter as "a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information" (Article 2(h)). The concept of "dissemination to the public" is further defined as "making information available, at the request of the recipient of the service who provided the information, to a potentially unlimited number of third parties" (Article 2(i)). Recital 14 further explains that "The mere possibility to create groups of users of a given service should not, in itself, be understood to mean that the information disseminated in that manner is not disseminated to the public. However, the concept should exclude dissemination of information within closed groups consisting of a finite number of pre-determined persons." It is the concept of "a finite number of pre-determined persons" that is unclear. Does this exclude all information on Facebook accounts that is shared with friends and that according to the privacy settings of the account holder is not visible to others? In this case, there is indeed a similarity between online posts and letters or phone calls, which are generally considered to be confidential. However, should there not be a critical number of "friends" or "group members" that leads to the loss of confidentiality protection and to the same treatment as offers to or information shared with the public in general?

Secondly, the DSA supports not only the detection of illegal information, but also the removal or disabling of access to illegal content. Prior permission of judicial or other competent authorities is not required. However, similarly to what is provided in the Platform to Business Regulation (P2B Regulation),[51] if the hosting provider decides to remove or disable access to specific items of information provided by the recipients of the service, it has to inform the recipient of the decision, at the latest by the time of the removal or disabling of access, and provide a clear and specific statement of the reasons for that decision. This statement of reasons needs to contain information on the redress possibilities available to the recipient of the service in respect of the decision, particularly through internal complaint-handling mechanisms, out-of-court dispute settlement and judicial redress (Article 15). Having an internal complaint-handling system is mandatory for online platforms, except when they qualify as micro or small enterprises within the meaning of the Annex to

[51] Art 4 Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services (P2B Regulation) [2019] PB L 186.

Recommendation 2003/361/EC (Articles 16 and 17). Recipients will also be entitled to select any duly certified[52] out-of-court dispute settlement body to resolve disputes relating to the removal or disablement of access, the suspension or termination of the recipient's account or of the provision of the service, in whole or in part, to the recipient. Online platforms have to engage in good faith with the selected body in view of resolving the dispute and they are bound by its decision. It is true that recipients remain free to apply for redress before the competent courts. However, it is likely that for many non-professional recipients the costs of judicial procedures will function as a disincentive. Dispute resolution is therefore likely to remain mainly in the hands of private actors. While it is understandable that an internal dispute resolution system is required, the question arises as to whether, particularly in cases where free speech is at stake, the facilitation of access to court proceedings through the introduction of harmonised rules limiting the costs of such proceedings would not be more suitable than the promotion of out-of-court dispute settlement.

A further example of outsourcing regulatory powers to private parties can be found in the rules applying to very large platforms. The proposal recognises that the potential to cause harm increases with the size of online platforms in terms of their number of users – their audience. In order to mitigate these risks, the DSA includes additional obligations for very large online platforms (those having 45 million or more average monthly active users in the EU).[53] One of the obligations imposed on such platforms is to carry out a yearly self-assessment of any significant systemic risks caused by their services and the use made thereof in the Union. The concept of "systemic risks" refers inter alia to the dissemination of illegal content, negative effects on human rights and intentional manipulation of their service (Article 26(1)). When systemic risks are identified, very large online platforms must take reasonable, proportionate and effective mitigation measures, such as adapting their recommender systems, reaching out to other private players, trusted flaggers[54] or other online platforms (Article 27). In addition, Article 28 requires very large online platforms to be subject to a yearly audit at their own expense to assess compliance with the specific obligations the proposal imposes on very large platforms, as well as any commitments undertaken under codes of conduct or crisis protocols. The identification and solution of risks is thus in the first instance left to the very large online platforms themselves, and compliance with their specific obligations is outsourced to private audit firms.

Requiring very large online platforms to carry out risk assessments themselves makes sense since they are the only entities that have full access to the data they collect and register on their users,[55] and they are often best placed to know the problems caused

[52] See on this point Art 18(2) DSA.

[53] Art 25 DSA.

[54] Pursuant to Recital 46, the status of a trusted flagger may and "should only be awarded to entities, and not individuals, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content, that they represent collective interests and that they work in a diligent and objective manner". Trusted flaggers can be public entities, such as Europol, but they can also be non-governmental organisations and semi-public bodies, such as the organisations that are part of the INHOPE network of hotlines for reporting child sexual abuse material.

[55] Even after opening itself up to academic scholars and journalists, Facebook's Crowd Tangle platform only allows access to a fraction of the total data Facebook operates with; see Facebook Crowd Tangle (*Facebook*, 17 January 2021) <https://www.crowdtangle.com>.

by their users and how to remedy them in the most cost-efficient way. Equally, it is understandable that the Commission wants the platforms themselves to bear the costs of inspecting compliance with the rules imposed by the DSA. The most critical point of mandatory audits by private, competing and profit-based audit firms is their independence towards the firms they audit – their clients. A reliable framework for "auditing the auditors" is therefore required. The DSA requires the organisations carrying out the audits to be independent from the very large online platform concerned, to have proven expertise in the area of risk management, to have technical competence and capabilities and to have proven objectivity and professional ethics, based in particular on adherence to codes of practice or appropriate standards (Article 28(2)). However, a specific supervisory framework for the auditors involved seems to be lacking. Nevertheless, very large platforms are required to provide the Digital Services Coordinator of their place of establishment or the Commission, upon their reasoned request and within a reasonable period specified in the request, access to data that are necessary to monitor and assess compliance with this Regulation (Article 31(1)). Upon request of the same entities, they also need to provide access to researchers meeting certain requirements for the sole purpose of conducting research that contributes to the identification and understanding of systemic risks (Articles 31(2) and (4)). Furthermore, Articles 41 ff DSA provide wide powers of investigation and remediation to the Digital Services Coordinators and the Commission, as we explore in Section V.

V. Digital enforcement

In its Chapter IV, the DSA outlines the proposed framework for implementation, cooperation, sanctions and enforcement. These activities can be referred to as "digital enforcement". *Lato sensu*, the need for digital enforcement signifies that means and mechanisms of enforcing the law in cyberspace need to be available just as they are in the real world.[56] *Stricto sensu*, digital enforcement refers to a growing field of public interest technology[57] aiming to use technology in order to facilitate the evidence-gathering process and/or the actions available to pursue certain remedies.[58] In the pursuit of this facilitation, the European Commission has already committed its support to the goal of "equipping law enforcement authorities with appropriate tools to ensure the security of citizens, with proper safeguards to respect their rights and freedoms".[59] The tools referred to by the Commission are so-called "AI tools" that could, for example, "help identify online terrorist propaganda, discover suspicious

[56] Eg see ME Kaminski, "An overview and the evolution of the Anti-Counterfeiting Trade Agreement" (2011) 21 Albany Law Journal of Science and Technology 412; A Ottolia and D Wielsch, "Mapping the information environment: legal aspects of modularization and digitalization" (2003–2004) 6 Yale Journal of Law & Tech 174, 247.

[57] Eg see B Schneier, Public Interest Tech (17 January 2021) <https://public-interest-tech.com>.

[58] Eg in the field of competition law, see M Verstager, "Competition in a digital age: changing enforcement for changing times" (*European Commission*, 26 June 2020) <https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/competition-digital-age-changing-enforcement-changing-times_en>.

[59] European Commission, "On Artificial Intelligence – A European approach to excellence and trust", White Paper, COM(2020) 65, p 2 final (*European Commission*, 19 February 2020) <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf>.

transactions in the sales of dangerous products, identify dangerous hidden objects or illicit substances or products, offer assistance to citizens in emergencies and help guide first responders".[60]

While several national public administration bodies already exist for the enforcement of obligations stemming from, for instance, media, consumer, competition or privacy law, the DSA proposes the creation of new national bodies tasked with the enforcement of the DSA itself. The procedural framework behind this body is laid out in Chapter IV of the DSA.

Article 38 indicates that Member States need to designate a Digital Services Coordinator that is expected to act independently from other public authorities or private parties (Article 39). The Digital Services Coordinator of a given Member State will enforce the DSA with respect to platforms that have their main establishment in the respective Member State (Article 40). Digital Services Coordinators have three types of powers (Article 40): investigation (eg retrieving evidence), enforcement (eg making compliance agreements, imposing fines and other interim measures) and additional powers that can kick in after their investigation and enforcement powers have been exhausted (eg applying for injunctions). In addition, the DSA sets up a European Board for Digital Services as an independent advisory group for national Digital Services Coordinators (Article 47) and gives the Commission further competences in the investigation of relevant conduct and the enforcement of sanctions as a form of enhanced supervision for very large online platforms (Article 51). Both Digital Services Coordinators and the Commission are given powers such as conducting on-site inspections, taking interviews and statements and requesting data from platforms. National Digital Services Coordinators may impose effective, proportionate and dissuasive penalties according to Article 42(2) of "6 % of the annual income or turnover of the provider of intermediary services concerned" (Article 42(3)). Platforms may also be sanctioned for submitting incorrect, incomplete or misleading information, for the failure to reply or to rectify this information, as well as for the failure to submit to on-site inspections. In these cases, penalties shall not exceed 1% of the annual income or turnover (Article 42(3)). The powers of the Commission to impose sanctions mirrors this structure (Article 59).

Chapter IV of the DSA outlines a complex interaction between national and European measures mandated by the regulation in the light of harmonising procedures and establishing cooperation where multiple stakeholders can participate in the enforcement of DSA violations. Administrative procedures aside, two points need to be kept in mind when looking at the DSA's digital enforcement approach as a whole: (1) the nature of investigations and enforcement on the digital single market; and (2) the readiness of Member States to comply with enforcement obligations stemming from the DSA.

Regarding the first point, it is important to realise how investigations and enforcement are expected to look with respect to the activity of platforms. Taking the example of the traceability of traders explored in Section II: a competent authority may issue an order in compliance with Article 9 DSA to a platform such as Instagram or TikTok, mandating the

[60] ibid.

disclosure of certain traders registered with the platform according to Article 22. This information may lead to evidence that does not need to be further analysed but rather used as such (eg the particular name of a trader). However, if, for instance, the information provided by the platform is a database of tens of thousands of traders, with the goal of understanding the scope of non-compliance with Article 22 DSA, public authorities will very likely be in a position where data analysis needs to be performed in order to lead to usable evidence. It is therefore imperative that public authorities responsible for the enforcement of the DSA are equipped with the internal or external infrastructure for undertaking such data analyses. In the field of consumer law, the Commission has already taken steps to promote cooperation in matters of what it calls "e-enforcement".[61] However, the more complex the data analysis becomes, the more we must acknowledge how far ahead the private sector, and especially very large platforms, will be in comparison with public authorities. For this reason, it is vital that public administration overcomes this disadvantage through collaborating with centres of excellence in interdisciplinary research in order to develop a sustainable and competitive framework of technology applicable to investigations and enforcement.

Moving to the second point, reflecting on the readiness of Member States to sustainably implement the frameworks indicated above, hasty and uncoordinated actions may very well lead to an inconsistent application of the DSA. Certain safeguards embedded in the DSA show that the Commission considered both the transnational effect of platform harms arising from platform activity as well as the efficiency gains in cooperation and technical assistance at the EU level.[62] To this end, it proposes in Article 67 the creation of a "reliable and secure" information-sharing system between Digital Services Coordinators that it would establish and maintain. Similarly, Article 45 sets up a new framework for cooperation between Member States, allowing them to communicate with Digital Services Coordinators from the jurisdiction of establishment in case there is a reason to suspect the existence of DSA infringements that the Member State in question would not have jurisdiction over. These provisions will hopefully alleviate the infrastructural differences between more and less digitalised Member States. Without such effective safeguards in place, the DSA would perpetuate some of the pitfalls of earlier regulation such as the UCPD, where considerable differences can be noted in national enforcement,[63] in spite of the pan-European presence of sufficient very large platforms that engage in the same behaviour across all Member States.[64]

[61] Consumer Protection Cooperation Network (*European Commission*, 17 January 2021) <https://ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/consumer_protection_cooperation_network/index_en.htm>.

[62] European Commission, supra, note 2, at 12.

[63] BEUC, "European Commission's report on the application of the Unfair Commercial Practices Directive" (*BEUC*, 24 June 2013) <https://www.beuc.eu/publications/2013-00457-01-e.pdf>.

[64] B Daigle and M Khan, "The EU General Data Protection Regulation: an analysis of enforcement trends by EU data protection authorities" (2020) Journal of International Commerce and Economics <https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement.pdf>.

VI. Conclusion

In this article, we endeavoured to conduct a first exploration of the DSA according to four points that stand out particularly from the perspective of consumer protection, a much-needed angle for the assessment of new platform responsibilities.

First, we discussed the internal coherence of EU law and looked at how the DSA does not fully align itself to earlier regulation on consumer protection relating to mandatory disclosures by traders who conclude online contracts with consumers. Second, regarding intermediary liability, the DSA mainly confirms the protection that the e-Commerce Directive offered intermediary service providers. In addition, it provides them with legal certainty that they will not suffer negative consequences from voluntary monitoring. Protection of the service recipients, in particular consumers or more general individuals, is mainly outsourced to private parties. Third, the enforcement of legal and self-regulatory norms is equally to a large extent outsourced to private entities, which raises concerns as to due process. Admittedly, Articles 41 ff DSA provide wide powers of investigation and remediation to the Digital Services Coordinators and the Commission. It remains to be seen whether this suffices to protect the interests of intermediary service recipients, in particular consumers. Lastly, we looked at digital enforcement and discussed the cooperation and EU assistance frameworks provided in the DSA. In the light of potential issues around the readiness of Member States to comply with DSA enforcement obligations from a technical perspective, the cooperation frameworks proposed by the DSA between Member States and with the Commission constitute much-needed support in making sure that digital asymmetry perils will not drastically affect the harmonising impact expected from the DSA.