UNIO - *EU Law Journal*. Vol. 7, No. 2, December 2021, pp 77-94.

School of Law – University of Minho

Taming Europe's digital landscape? Brief notes on the proposal for a Digital Services Act

Miguel Pereira*

ABSTRACT: In light of the intensive technological developments in the last two decades that we have borne witness to, the European Union is looking to modernise its framework governing the provision of digital services within the Single Market. The main regulatory instrument, in this regard, is the E-Commerce Directive enacted 20 years ago, which focuses on ensuring freedom of movement of goods and services. The evolution of the information society, towards "attention economy" services, has, however, brought to light the deficiencies of a markedly liberal approach to the Single Digital Market's ("SDM") Regulation. The main instrument to modernise the SDM's Regulation is the Digital Services Act ("DSA") which introduces new responsibilities on service providers in an attempt to better safeguard the EU citizen's safety and fundamental rights online. In this paper, we review the Commission's proposal for the DSA, highlighting the main novelties the instrument introduces and the main issues we have identified so far.

KEYWORDS: Digital Services Act – Digital Single Market – online platforms – internet governance.

* Master's student in European Union Law at the School of Law of the University of Minho.

1. The E-Commerce Directive's 20th anniversary and the need to shape Europe's digital future

20 years following the adoption of the E-Commerce Directive,[1] the European Union ("EU") is looking to modernise its regime governing the provision of intermediary services online. This initiative follows two decades of intense technological development from which numerous innovative digital services emerged, some of which appear to be at the outskirts of the space that the E-Commerce Directive set out to regulate but have, nevertheless, assumed a pivotal role in the digital economy. A few of those service providers have become so immense that they have, in essence, become gatekeepers, raising concerns about the fairness of the digital market and its accessibility to newcomers.[2] Their all-encompassing influence is not limited to the market's functioning but has extended to many of our most basic daily interactions (from shopping to sharing information, to learning and debating all manner of issues), leading some authors to recognise a quasi-public nature to these online spaces.[3] Notwithstanding that, they remain scarcely regulated. This lack of regulation has meant that the efforts to counteract the spread of illegal content and disinformation or to ensure the protection of fundamental rights online have been largely led by the service providers themselves, through their terms of services – resulting in uneven measures and safeguards.[4]

It is against this backdrop that the European Commission put forth a proposal for a Digital Services Act ("DSA"),[5] seeking to amend certain provisions of the E-Commerce Directive and to impose *ex-ante* rules on very large online platforms. The Proposal is in line with the Commissions' Shaping Europe's Digital Future communication and was presented following the approval of three European Parliament resolutions.[6] The intent is for the Regulation to be an overarching framework covering all providers of intermediary services, laid out in terms that address current necessities and pave the way for the development of new technologies, eliminating barriers to the proper functioning of the Digital Single Market and ensuring a safe, predictable, and trusted online environment. The DSA builds on the framework put in place by the

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Shaping Europe's digital future, COM/2020/67 final, 8, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0067&qid=1622538522938&from=EN.

[3] Giovanni De Gregorio, "From constitutional freedoms to the power of the platforms: protecting fundamental rights online in the algorithmic society", *European Journal of Legal Studies*, v. 11, no. 2 (2019): 79-89.

[4] Jack M. Balkin, "Free speech in the algorithmic society: big data, private governance, and new school speech regulation", *U.C. Davis Law Review*, v. 51, no. 3 (2018): 1183-1184.

[5] European 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 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en.

[6] European Commission, COM/2020/67 final; European Parliament, Resolution on improving the functioning of the Single Market (2020/2018(INL)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html; European Parliament, Resolution on adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0273_EN.html; European Parliament, Resolution on the Digital Services Act and fundamental rights issues posed (2020/2022(INI)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0274_EN.html.

E-Commerce Directive, leaving its core principles untouched, such as the freedom to provide services in the Union [Article 3(2) E-Commerce Directive], the Internal Market clause [Article 3(1) E-Commerce Directive], the conditional exemption from liability for intermediary service providers, and the prohibition on general monitoring obligations – the latter two are, however, intended to be moved to the DSA.

The purpose of this paper is to provide an overview of the DSA, as proposed by the Commission, making note of the changes to the E-Commerce principles it introduces, the incorporation of the Court of Justice of the European Union's ("CJEU") case law, and the difficulties we have identified so far. The analysis is not an exhaustive one but rather focuses on the main aspects of the proposal.

2. Scope of the Digital Services Act

With a view to addressing the increasing fragmentation of the regulatory landscape governing digital services, as well as fostering an auspicious environment for the flourishing of innovative digital services, while promoting and protecting fundamental rights, the DSA intends to lay down the ground rules for the provision of digital intermediation services within the Single Market. In that sense, and according to its Article 1(1), its material scope covers:

i. the conditional exemption from liability of providers of intermediary services, building on the regime introduced by the E-Commerce Directive;

ii. due diligence obligations impending on digital intermediation service providers;

iii. implementation, enforcement, and supervision of compliance with the obligations laid out in the DSA.

As for the subjective scope, the DSA applies to all providers of intermediary services that provide services to recipients that have their place of establishment or residence in the EU, regardless of the place of establishment of the provider. Intermediary services are defined in Article 2(f) as: (i) mere conduit services (*i.e.* Internet Service Providers); (ii) caching services; and (iii) hosting services. Similar to the regime governing the exemption of liability of providers of intermediary services (*vide infra* section 3), the Commission has opted to keep the E-Commerce Directive's concepts and definitions for these services, presumably due to concerns with maintaining legal certainty, as expressed by the European Parliament,[7] which accounted for the fact that a number of EU legislative instruments, administrative acts, and private contracts rely on the definitions laid out in the E-Commerce Directive. Notwithstanding this, the DSA seeks to address, at least in part, the debate on whether certain content hosting providers, which play an active role in the content provided by the recipients of the service, should be considered as hosting services for the purpose of being covered by the exemptions of liability provided for by the E-Commerce Directive.[8] The DSA seems to try to address the E-Commerce Directive's shortcomings in this regard by:

i. clarifying the legal relevance attributable to a voluntary active role as regards illegal content (*vide infra* section 3);

ii. including the sub-category "online platform", distinguishable from the

[7] European Parliament, Resolution [2020/2018(INL)], paragraph 11.

[8] See, *inter alia*, Eleonora Rosati, "Why a reform of Hosting Providers' safe harbour is unnecessary under EU Copyright Law" (Create Working Paper 2016/11, 2016), accessed May 26, 2021, https://dx.doi.org/10.2139/ssrn.2830440, and Thomas Margoni, "Did anybody notice it? Active and passive hosting in Italian case law on ISP liability", *Kluwer Copyright Blog*, May 11, 2012, http://copyrightblog.kluweriplaw.com/2012/05/11/did-anybody-notice-it-active-and-passive-hosting-in-italian-case-law-on-isp-liability/.

standard hosting service by the additional requirement of dissemination to the public of the hosted information provided by the recipient of the service, at the latter's request;[9] and,

iii. instituting a specific regime for this sub-category of service providers (*vide infra* sections 4.2 and 4.3).

It should also be noted that the Commission decided to clearly define the situations in which a service provider is to be considered as offering a service in the Union, something that the E-Commerce Directive failed to do. In that sense, a service provider is considered to be offering services in the EU whenever natural or legal persons, in one or more Member States, are able to use its services and the service provider has a substantial connection to the EU – to be assessed in light of specific factual criteria, such as a significant number of users in one or more Member States or the targeting of activities towards one or more Member States. This last element is not only a recognition of the Court of Justice of the European Union's ("CJEU's") *Pammer* case law[10] but an alignment with the General Data Protection Regulation ("GDPR").[11]

3. Conditional exemption from liability of providers of intermediary services and prohibition of general monitoring obligations

In respect to the exemption of liability of providers of intermediary services and the prohibition of general monitoring obligations, the DSA keeps the framework put in place by the E-Commerce Directive, seeking essentially to move it from the context of this Directive to the proposed Regulation. The compilation of these rules in the context of the DSA is adequate as, if and when approved, it will become the main instrument to address illegal content online, a matter that is intimately connected with the liability exemption. The rules set out in Chapter II of the DSA, namely Articles 3 through 7, safeguard intermediaries from liability regarding the transmission of illegal content, information, or activities by the recipients of their services – also known as "*secondary liability*".[12]

[9] The choice of such a wide designation is likely meant as an umbrella term capable of encompassing a multitude of services with different characteristics, which, nonetheless, meet the basic requirements we have highlighted.

[10] Judgment of 7 December 2010, *Pammer*, Joined cases C-585/08 and C-144/09, ECLI:EU:C:2010:740, paragraphs 92-94.

[11] While the regulation does not put forward a definition for the "offering of goods or services" in the EU, its Recital 23, which advances some clues as to what elements should be considered to establish this criterion, has been interpreted by the European Data Protection Board as reflecting the CJEU's *Pammer* case law. European Data Protection Board, "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation", https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en. For an overview of the concept of "targeting of activities" and its use in EU law, including in the context of the GDPR, see Aurelio López-Tarruella Martínez, "El criterio de las actividades dirigidas como concepto autónomo de DIPR de la Unión Europea para la regulación de las actividades en internet", *Revista Española de Derecho Internacional,* v. 69, no. 2 (2017), http://dx.doi.org/10.17103/redi.69.2.2017.1.09.

[12] Giovanni Sartor, "Providers liability. From the eCommerce Directive to the future" (In-depth analysis for the IMCO Committee, 2017), accessed May 26, 2021, https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2017)614179. The author reviews the existing liability regime for intermediary service providers, adducing arguments for and against such liability.

The existing framework is known as the "*safe harbour*" regime and exempts intermediary service providers from liability, provided that they act in a passive manner in relation to the content that is transmitted, stored, or hosted and that, upon obtaining knowledge or awareness of illegal content, they act expeditiously to remove or disable access to such content.[13] While there seems to be widespread support for the continuance of this regime, there is also convergence around the need to update it to better address emerging technologies.[14]

3.1. Exemption of liability of intermediary service providers in the DSA and the good Samaritan clause

The only change to note relating to the rules governing the exemption of liability of mere conduit and caching services is the amendment of the wording of the provisions, by comparison to the E-Commerce Directive, which required Member States to adopt specific provisions of national law to transpose the instrument – made redundant as the DSA is drafted as a Regulation, not a Directive. As for hosting services, two amendments can be noted: (i) Article 5(1)(a) replaces "*information*" with "*illegal content*" [by comparison to Article 14(1)(a) E-Commerce Directive]; and (ii) the introduction of an additional paragraph [Article 5(3)] regarding platforms that allow consumers to conclude distance contracts with traders (*i.e.* online marketplaces). This provision clarifies that online marketplaces are not exempted from liability whenever the information, or the way that the transaction is enabled, leads the consumer to believe that the information, product, or service is provided by the platform itself or by a recipient of the service acting on behalf of the platform. Finally, Article 5(4) eliminates the reference to the Member States' capacity of establishing procedures governing the removal or disabling of access to information (in the context of orders by administrative or judicial authorities requiring the service provider to terminate or prevent an infringement) previously required by the E-Commerce Directive, as these procedures will be governed by the DSA.

The biggest novelty in this context is the recognition, in Article 6, of a provision, seemingly inspired by the good Samaritan clause of the US's Communications Decency Act,[15] safeguarding providers of intermediary services which, of their own initiative, conduct investigations or other activities aimed at detecting, identifying, and removing illegal content, by asserting that these activities are without prejudice to their eligibility for the exemptions from liability contained in the preceding Articles. In a recent judgment, the CJEU addresses this question in a manner that seems to confer a stronger protection than that which would be afforded by Article 6 DSA.

While the DSA provides cover only for investigations and other activities aimed at detecting illegal content, in the recent judgment in *Youtube and Cyando*, concerning hosting service providers, the Court seems to extend this protection to other activities not specifically carried out in order to detect illegal content but rather at curating content published on online platforms, by stating: "*the fact that the operator of an online content-sharing platform automatically indexes content uploaded to that platform, that that platform has a search function and that it recommends videos on the basis of users' profiles or preferences is not a sufficient ground for the conclusion that that operator has 'specific' knowledge of illegal activities carried*

[13] Eleonora Rosati, "Why a reform of Hosting Providers' safe harbour is unnecessary under EU Copyright Law", 2.
[14] European Commission, COM(2020) 825 final, 9.
[15] Giovanni Sartor, "Providers Liability. From the eCommerce Directive to the Future", 17.

out on that platform or of illegal information stored on it".[16] The Court then goes on to reaffirm that the exemption from liability falls only when the host service provider plays an active role of the kind that would give it knowledge or control over the content its users upload,[17] something which would only be possible if it engaged in general monitoring of the content being uploaded to its platform – an obligation which cannot be imposed on service providers.[18] With this passage the Court addresses one of the main controversies surrounding the liability shield for hosting service providers, though it should be noted that the CJEU introduced in paragraph 59 of the ruling a disclaimer stating that the interpretations it carried out in the course of the present review do not concern Article 17 of Directive (EU) 2019/790 of the copyright and related right in the Digital Single Market ("CDSMD"),[19] an Article that has increased the tension between the prohibition on general monitoring obligations and the protection of copyright holders' rights, as we will discuss in the next section. Considering that the Commission's proposal for the DSA predates the issuance of the judgment in *Youtube and Cyando*, and that the legislative process is still in its early stages, it will be interesting to discover if and how the legislator will try to incorporate this case law in the final text of the Regulation.

3.2. Prohibition of general monitoring obligations and orders from national judicial and administrative authorities

The extent of the prohibition of general monitoring obligations remains a contentious issue, with differing views on its applicability as concerns specifically identified rights or previously identified illegal content (with further ramifications appearing when considering the necessity or not of a judicial or administrative order) – though the CJEU has recently expanded its case law towards a less restrictive approach in the context of injunctive orders relating to defamation cases. The DSA does not introduce significant changes to the wording of the provision governing this prohibition, the most notable one being the removal of the possibility for Member States to require service providers to promptly inform competent authorities of alleged illegal activities or content undertaken or provided by recipients of the service or to oblige them to provide competent authorities with information on the identity of recipients of the service with whom they have storage agreements (as the DSA establishes rules for such procedures).

The issue revolves around the scope that should be attributed to Recital 47 E-Commerce Directive and, respectively, Recital 28 DSA, where they state that the prohibition of general monitoring obligations does not extend to monitoring obligations "*in a specific case*". While the CJEU has generally avoided tortuous inroads into the matter, preferring to stand by an interpretation that left little room for the imposition of monitoring obligations of any kind, it recently recognised, in *Glawischnig-Piesczek*,[20] the possibility of imposing (court-ordered) monitoring obligations on

[16] Judgment of the Court of 22 June 2021, *Youtube and Cyando*, Joined Cases C-682/18 and C-683/18, ECLI:EU:C:2021:503, paragraph 114.

[17] *Youtube and Cyando*, Joined Cases C-682/18 and C-683/18, paragraph 117.

[18] *Youtube and Cyando*, Joined Cases C-682/18 and C-683/18, paragraph 113. This is true as regards the E-Commerce Directive and, as we will highlight, as regards the DSA.

[19] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

[20] Judgment of the Court of 3 October 2019, *Glawischnig-Piesczek*, C-18/18, ECLI:EU:C:2019:82,

content that is identical or equivalent to a specific piece of defamatory content previously declared to be unlawful. The problem lies in the lack of guidance as to the approach hosting service providers should follow to heed these court orders without encroaching on users' fundamental rights and without such an order resulting in a general monitoring obligation regarding all content uploaded to their platforms.[21] As Senftleben and Angelopoulos point out, if, for defamation, this seems, at least conceptually, possible, due to the specificity of the context in which defamatory content must be reproduced (which should avoid a great number of re-postings of identical or equivalent content) and the absence of a risk of requests to monitor for "*long lists of rights*" held by rightsholders in this area, the same cannot be said for other types of unlawful content, namely in the copyright arena. The hope, expressed by the authors, that the DSA would help clarify the legal framework resulting from the interplay of the prohibition of general monitoring obligations, the CDSMD and the *Glawischnig-Piesczek* case law seems to have been unfounded.[22]

Rather than address the persisting issues regarding general monitoring obligations, the DSA focuses on regulating the procedure for national authorities to order service providers to act against illegal content (Article 8) or to provide information about one or more specific individual recipients of the service (Article 9). These provisions focus mainly on establishing standard information obligations for competent authorities to transmit to service providers along with the orders, communication of these orders to Digital Services Coordinators ("DSCs") of other Member States and, in the context of orders to act against illegal content, the territorial scope of such orders – an issue that will deserve the upmost attention given the fact that content might be deemed as illegal on the basis of national law.

4. Due diligence obligations impending on providers of intermediary services

By reference to the two main aims of this Regulation, improving the functioning of the Internal Market in the context of digital services and ensuring a safe and transparent online environment, Recital 34 identifies the need to set clear, balanced, and harmonised obligations for providers of intermediary services. Considering the diverse range of services that are intended to be governed by its provisions, however, the DSA puts forth a general framework applicable to all intermediary services and different rule sets designed according to the type of provider that falls within its remit and, as regards online platforms, their size.

The general set of rules applicable to all providers of intermediary services is laid out in Articles 10 to 13 and focuses on minimum requirements for communication and transparency. As regards communication requirements, Article 10 mandates the service providers to designate a single point of contact for the purpose of communications with the Commission, Member States' authorities and the European Board for Digital Services ("Board"), requiring the information on its identity and

paragraph 53.

[21] Martin Senftleben and Christina Angelopoulos, "The Odyssey of the prohibition on general monitoring obligations on the way to the Digital Services Act: between article 15 of the e-Commerce Directive and article 17 of the Directive on copyright in the digital single market" (Paper, University of Amsterdam, 2020), 7-18, accessed May 26, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717022.

[22] Martin Senftleben and Christina Angelopoulos, "The Odyssey", 29-34.

means of communication to be made publicly available, and setting requirements as to the languages for communication. Article 11 requires that service providers which do not have an establishment in the EU but which offer services in the Union (*vide supra* section 2) to designate a legal representative in one of the Member States where it offers its services, which should be mandated with sufficient powers and resources to communicate and cooperate with the Commission, Member States' authorities and the Board on matters related to compliance with the DSA. Something to note is that the legal representative can be held liable for non-compliance with this Regulation. Concerning transparency obligations, Article 12 requires service providers to set out in their terms and conditions, in clear and unambiguous language, any conditions that they impose on the recipients' ability to provide information, as well as on policies, procedures and tools used for content moderation, including on algorithmic decision-making and human review. In exercising these restrictions, service providers must act in a proportionate, objective, and diligent manner with due regard to the interests at hand and the fundamental rights contained in the Charter. Finally, Article 13 requires all service providers that are not micro or small enterprises[23] to publish, on a yearly basis, transparency reports on any content moderation they might have engaged in along with a set of standardised information on that activity.

4.1. Rules applicable to hosting service providers

The rules applicable to all hosting service providers are covered by Articles 14 and 15 and mandate these providers to put in place notice and action mechanisms by which any individual or entity may notify them of the presence of specific items of information that they deem to be illegal content. These notices must contain an explanation of the alleged illegality, the URL of the piece of information, contact info of the individual or entity submitting the notice (except when the notice regards offenses related to sexual abuse or exploitation of minors and child porn), and statement of good faith by the notifier – an attempt to address the issue of false notices. In terms of the content of the notice, this Article closely follows the European Parliament's text in its request for a proposal for a Regulation on contractual rights as regards content management.[24] Something to note, in the context of the "*safe harbour*" rules, is that a notice containing the above-mentioned elements is sufficient for the provider to be considered as having actual knowledge or awareness of the illegal information. The service provider is required to provide the notice-giver with feedback regarding the information flagged by them and to highlight the available redress mechanisms to contest the decision taken by the provider.

In what regards removal or disabling of access to content, as per Article 15, service providers are required to notify the recipient of the service of the decision to remove or disable access to the content, at the latest at the time of execution of the decision. This notification must be accompanied by a statement of reasons that informed the decision which should contain, among other elements: the territorial

[23] An enterprise's classification as micro or small is to be assessed following the rules set out in the Annex to the Commission's Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises. Micro enterprises must employ fewer than 10 persons and have an annual turnover or balance sheet not exceeding 2 million EUR. Small enterprises must employ fewer than 50 persons and have an annual turnover or balance sheet not exceeding 10 million EUR.
[24] European Parliament, Resolution (2020/2019(INL)), particularly Article 9 of the text proposed in the Annex.

scope of the decision, information on the use of automated means in taking the decision (including when automated means were used to detect or identify the content), explicit reference to the legal grounds or contractual terms (in those cases where the decision is based on the terms of service) on which the decision was taken with accompanying information on the rationale that informed it, and information on the available redress mechanisms.

In attendance to transparency and legal certainty in the context of content moderation, service providers are required to register these decisions in a publicly accessible database managed by the Commission – a welcomed initiative which should increase the users' capacity to understand the rationale behind content moderation engaged by hosting platforms and which will certainly prove useful for the exercise of the redress possibilities. Additionally, the academic community will benefit from greater insight into content moderation practices.

4.2. Rules applicable to online platforms

As we have highlighted already, the DSA intends to create specific obligation for online platforms – hosting services which disseminate to the public information provided by the recipient of the service, at their request. Section 3 of Chapter III institutes the rule set for these service providers, excluding from its remit, micro and small enterprises. With a view to level the playing field between users and online platforms, the DSA obliges them to create internal mechanisms to address claims raised against decisions made by them, creates new rights for the service recipients, and institutes specific transparency obligations. Attention should also be drawn to the role of "trusted flaggers" whose notices submitted under Article 14 should be treated with priority[25] and to the requirement that online platforms inform law enforcement or judicial authorities of suspicions of serious criminal offenses involving the threat to the life or safety of persons. A final preliminary note should also be made to the fact that recipients that frequently provide manifestly illegal content should be suspended.[26] Additional responsibilities impend on very large online platforms ("VLOPs") which we will cover in the next section.

Article 17 requires that online platforms set up complaint-handling systems that should be free of charge and allow for complaints to be filled electronically, in an easily accessible and user-friendly format, against decisions to remove or disable access to content, suspend or terminate the provision of services to recipients (in whole or in part), as well as those that suspend or terminate the recipient's account. Should the complaint contain sufficient elements to allow the online platform to consider that the information is not illegal (or incompatible with its terms and conditions) or that the conduct of the recipient does not warrant the suspension or termination of the service or account, the online platform should reverse its decision without undue delay. In line with GDPR principles, the decisions regarding those complaints cannot be taken solely based on automated means – as opposed to the initial decision to which

[25] Trusted flaggers must meet the following cumulative requirements: have particular expertise in detecting and notifying illegal content, they must be independent and represent collective interest, and they must carry out their activities diligently and objectively. This status is granted and may be revoked by the DSC of establishment.

[26] As for individuals or entities that frequently submit manifestly unfounded notices or complaints, online platforms should suspend, for a reasonable period of time, the processing of notices or complaints submitted by them. The rules governing the suspension of services or the processing of notices/complaints should be clearly laid out in the terms and conditions of the online platform.

the complaint refers to, for which there is no such prohibition (*vide supra* subsection 4.1). The decisions taken in the context of Article 17 can be the subject of out-of-court dispute settlement at the request of the recipient. The out-of-court dispute settlement must be conducted by a body certified by the DSC of establishment which must meet certain conditions for the certification – *inter alia*: it must be independent, have sufficient expertise in issues arising from illegal content or terms and conditions, and be easily accessible through electronic means of communication.

As for provisions targeting online marketplaces, Article 22 requires that these platforms conduct prior due diligence on traders, establishing the minimum elements that need to be collected to properly identify them and obliging the platforms to make reasonable efforts to assess whether the information provided is accurate through reliable public sources. Some of the elements provided by the trader and verified by the platform should be made available to consumers, namely identification and contact information, required licensing information (when applicable), the trade register and registration number of the trader, as well as self-certification of compliance with applicable EU law.

Finally, additional transparency obligations arise from the DSA for online platforms. On the one hand, additional information must be added to the transparency report submitted pursuant to Article 13 concerning, namely, performance indicators connected to disputes brought before the out-of-court dispute settlement bodies, suspensions imposed in the context of Article 20, and any use of automated means for the purpose of content moderation, along with details on their purpose, accuracy, and safeguards in place.[27] On the other hand, online platforms will have to ensure that the recipients of their services can identify, in a clear and unambiguous manner and in real time, for each specific advertisement that is displayed:

i. That the information is an advertisement;

ii. The natural or legal person on whose behalf the advertisement is displayed; and,

iii. Meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed.

While greater transparency is indeed achieved, the DSA stops short of specifying that this information should be clearly noticeable when viewing the advertisement or of granting the recipient the right to opt-out of targeted advertising in general and, in particular, advertisement based on pervasive tracking, notwithstanding the fact that the European Parliament had called on the Commission to regulate targeted advertisement in a stricter manner, in comparison to other forms of advertisement, and expressed its view that this type of advertisement should be conditional on users' freely given, specific, informed and unambiguous consent.[28] In a related matter, the Commission has recently put forth an initiative to introduce legislation regarding political and issues-based advertisement. The public consultation was conducted during the course of 2021 and the Commission is expected to introduce a proposal for a legislative instrument governing this type of advertisementsduring the year.[29]

[27] Online platforms are additionally required to publish and communicate to the DSC of establishment, every six months, the average monthly active users of their service.

[28] Resolution 2020/2019(INL), paragraph 14.

[29] See, "Political advertising improving transparency", accessed November 24, 2021, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12826-Political-advertising-improving-transparency_en.

4.3. Additional obligations applicable to very large online platforms

One of the guiding principles of the DSA is the differentiation of the regimes applicable to digital services based on the size and specific risks that they represent. This is an effort to address the highest risks identified in the current landscape, while trying to avoid a chilling effect on the emergence and development of new technologies and players in the market. On specific due diligence obligations, the DSA distinguishes VLOPs from the remaining intermediary services and, in particular, online platforms, due to their size, risk, and financial capability and Section 4 of Chapter III, therefore, imposes additional obligations on them. VLOPs are online platforms with an average number of monthly users equal to or greater than 45 million – this number is tied to the EU's population and should be adjusted when necessary, via a delegated act, so that it reflects 10% of the population at all times. The status of VLOP is attributed by the DSC through the establishment of the service provider, subject to an assessment every six months and, should the number of average monthly users drop below the limit set in the DSA or in subsequent delegated acts, may be rescinded – the DSC of establishment must transmit this information to the Commission so that the latter may publish an updated list in the Union's Official Journal (the effects of the designation, or termination thereof, apply from four months after the publication).

VLOPs will be expected to conduct a yearly risk assessment with the aim of identifying the systemic risks stemming from the functioning and use of their services in the EU. The risk assessment must reflect, at least, the risk their service poses as regards dissemination of illegal content, negative effects for the exercise of fundamental rights, and the intentional manipulation of their service with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or on electoral processes and public security (Article 26). VLOPs must also consider how their content moderation, recommender systems, and advertisement systems impact those public goods. To address these risks, VLOPs must put in place reasonable, proportionate, and effective mitigation measures, specifically designed to address the identified issues. Such measures may focus, *inter alia*, on adapting content moderation and recommender systems, decision making processes, terms and conditions, or involve the limitation of the display of advertisements, initiation of cooperation with trusted flaggers and the adherence to codes of conduct or crisis protocols in the context of Articles 35 to 37. In this regard, VLOPs will necessarily have to submit themselves, on an yearly basis and at their expense, to an independent audit that will assess the compliance with the obligations set out in Chapter III of the DSA, as well as with the voluntary commitments undertaken in the context of the aforementioned codes of conduct (including on online advertisement, pursuant to Article 36) and crisis protocols.

In terms of content curation, Article 29 requires that VLOPs set out in their terms and conditions, in a clear, accessible, and easily comprehensible manner, the main parameters used by their recommender systems – to be understood as those systems that suggest, in the VLOPs' interface, information to the recipient of the service, including as a result of a search initiated by the user, or by otherwise determining the relative prominence of information in the interface [Article 2(o)]. In addition to the obligation to inform on the functioning of recommender system, VLOPs must list the options made available to the recipient to modify or influence said parameters, including at least one that is not based on profiling. The possibility of switching between recommender systems should be included in the interface in an easily accessible

manner that allows recipients to amend their preference for recommender system at all times. While empowering the user to opt out of profiling-based recommender system, the DSA, does not go as far as to make those recommender systems (based on profiling) subject to an opt in requirement, presumably in attendance to the central role that they play in the business model of many of these platforms. While we must concede that introducing an opt in requirement could potentially have a financial impact on these platforms (an element that would need to be confirmed by the relevant impact assessments), subjecting content curation to the users' clearly stated preference would reinforce their fundamental rights protections and grant the user's greater control over their interactions with these platforms.[30]

VLOPs are also subject to additional transparency requirements concerning advertisement and transparency reports. Article 30 obliges VLOPs to compile and make publicly available a database covering all advertisements displayed on their interfaces (the record of each advertisement should be kept up to one year after it was displayed for the last time), containing information on the content of the advertisement, the natural or legal person on whose behalf it was published, whether the advertisement targeted a specific group of recipients and the main parameter to determine such group, as well as the total number of users reached by the advertisement. These obligations are in addition to the ones detailed above in subsection 4.2. As for transparency reports, Article 33 requires that VLOPs publish the report envisaged by Article 13 every six months (as opposed to the yearly reports for online platforms). In addition to that, at least once a year, they must make publicly available a report with the results of the risk assessment and related risk mitigation measures (identified and implemented), as well as the audit report and the accompanying audit implementation report. Still in the context of transparency, Article 31 sets out specific procedures for access by the DSC of establishment or the Commission, as well as vetted researchers. This is particularly relevant given that, at present, the decision on which researchers get access to data, and the data they get access to, is exclusively in the hands of VLOPs. As the Commission notes in its assessment of the Code of Practice on Disinformation,[31] under which large online platforms entered commitments to empower the research community, this has resulted in arrangements that are discretionary and multi-bilateral, as opposed to "*open and non-discriminatory approaches empowering a larger, multi-disciplinary community of researchers*". The Commission noted, additionally, issues with the quality of the datasets as well as with the interfaces put in place to access the data.[32] The inclusion of this provision, and the related rules of access to be set out by the Commission, will hopefully contribute not only to greater access, but to more widespread and independent analysis, as well as consistency in the data that is furnished.

A final note should be made regarding the role of the compliance officers, which are responsible for the cooperation with the DSC of establishment and the

[30] As the European Data Protection Supervisor ("EDPS") supports in his opinion. European Data Protection Supervisor, Opinion 01/2021 on the Proposal for a Digital Services Act, paragraph 32, https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf.

[31] "EU Code of Practice on Disinformation", accessed November 24, 2021, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454.

[32] European Commission Staff Working Document, Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement (SWD(2020) 180 final), 11, accessed November 24, 2021, https://ec.europa.eu/transparency/documents-register/api/files/SWD(2020)180_0/de00000000002265?rendition=false.

Commission, coordinating the activities relating to the audit report, informing and advising management and employees of the platform, and monitoring the compliance of the VLOP with its obligations under the DSA (Article 32). The compliance officer must be provided with all the resources necessary to carry out these tasks and must report to the highest level of management of the platform.

5. The Digital Services Coordinators and the European Board for Digital Services

The DSC is the competent national authority for the application and enforcement of the DSA. Member States may appoint more than one competent authority for this purpose (provided the tasks attributed to each are well defined) but should designate one as the DSC – which will, in this event, be responsible for ensuring the coordination of those entities at a national level, in what concerns the application of the DSA. The DSC must be an independent authority and cannot take instructions from any other public authorities or private entities.

Providers of intermediary services are subject to the jurisdiction of the Member State in which they are established or where their designated legal representative is established or resides. In the event that a service provider fails to appoint one, all Member States have jurisdiction – should one exercise such jurisdiction, must promptly inform all other Member States and ensure adherence to the *ne bis in idem* principle (Article 40).

Article 41 establishes the minimum investigatory and enforcement powers that the DSC should be endowed with. DSCs should be able to ask information from service providers on suspected infringements of the Regulation (as well as any person acting in a professional capacity that may reasonably be aware of such infringements), to conduct on-site inspections and seizure of information, and to interrogate members of staff or representatives of the services provider (or those persons acting in a professional capacity). DSCs must also have the power to accept commitments from intermediary service providers, to order the cessation of infringements as well as proportionate remedies, to impose fines and periodic penalty payments for failure to comply with any order to cease the infringement or to cooperate with an order issued within the exercise of the DSCs investigatory powers. Should these measures fail, in the face of a persisting infringement which causes serious harm which cannot be avoided through the exercise of other powers, the DSC shall require that the management body of the service provider submit an action plan contemplating measures to terminate the infringement. If it considers that the measures contemplated by the management board are not sufficient, that the infringement persists and causes great harm, entailing a serious criminal offense involving a threat to life or safety of a person, it may request the competent judicial authority to restrict access by the recipients concerned by the infringement (or when such is not technically feasible) to the entire online interface of the service provider. The restrictions last four weeks but can be prorogated depending on judicial authorisation (which, nevertheless, should establish the maximum number of prorogations). However, the DSC can only resort to this possibility after having invited all interested parties to submit written submissions, allowing a period of submission that should never be less than two weeks. Considering that this solution is only available for serious criminal offenses which endanger the life and safety of persons, a process involving a wait period of two weeks before judicial action might be requested seems especially lacking, in the

face of the urgency it looks to address – particularly if we consider that a competent judicial authority would be involved in the assessment of the interests and rights at issue, not a private entity.

Penalties in the context of the DSA must be effective, proportionate, and dissuasive. Penalties imposed for failure to comply with obligations laid down in the Regulation had a maximum amount set at 6% of the annual income or turnover of the service provider, whereas penalties for the supply of incorrect, incomplete or misleading information, failure to reply or rectify incorrect, incomplete or misleading information and to submit to an on-site inspection shall not exceed 1% of the annual income or turnover. Periodic penalty payments, on the other hand, are capped at 5% of the average daily turnover of the provider, based on the information of the preceding financial year.

If the DSC suspects that a provider, over which it does not have jurisdiction, is infringing its obligations under the DSA, it may request the DSC of establishment to take the necessary investigatory and enforcement measures. The same applies to the Board when the infringement affects at least three Member States. The DSC of establishment has two months to assess the situation and communicate its decisions to the DSC that referred the matter (or the Board, as it may be). Where the DSC of establishment fails to provide feedback within that timeframe, the DSC that referred or the Board may request the Commission to assess the matter – the Commission then can request the DSC of establishment to reassess its position (Article 45). DSCs may also conduct joint investigations on service providers operating in several Member States and may request the Commission to investigate when it has reason to believe that a VLOP infringed the DSA (Article 46).

Article 47 establishes the Board as an advisory group composed of the national DSCs with the main objective of advising the DSCs and the Commission on a consistent application of the DSA, effective cooperation between DSCs, contributing with guidance and analysis and assisting DSCs and the Commission on the supervision of VLOPs. Its main tasks are (Article 49): supporting the coordination of joint investigations and issuance of opinions, recommendations, or advice to DSCs.

6. Supervision of very large online platforms

The supervision of VLOPs' compliance with the special obligations imposed on them is ensured through a mixed system, lead at a first stage by the DSC of establishment and, at a second stage, by the Commission – if the VLOP fails to remedy its infringement upon the request and under the guidance of the DSC of establishment. As a preliminary note, we should point out that the wording of Article 50(1) suggests that the enhanced supervision process described in the present section is only applicable in cases of suspected infringements of the special obligations on VLOPs, pursuant to Section 4 of Chapter III (*vide supra* section 4.3), and not to infringements of the general obligations imposed on all online platforms. This system is governed by the provisions in Section 3 of Chapter 4.

The DSC of establishment may adopt a decision finding that a VLOP has infringed one or more of the special provisions applicable to it, at which stage the DSC of establishment shall ask the platform to submit, within one month from the decision of infringement, an action plan detailing how it intends to terminate or remedy the infringement (this action plan should be simultaneously communicated

to the Board and the Commission).[33] The Board, within one month of receipt of the action plan, must draft an opinion on the same and transmit it toto the DSC of establishment, which will then decide whether the action plan is appropriate or not to terminate or remedy the infringement (also within one month). Should the DSC of establishment have doubts about the VLOP's ability to terminate or remedy the infringement, it may request the platform to submit itself to an additional independent audit. At this stage, following the different timelines established in Article 50(4) (conditional on the performance or not of an audit or the VLOP's failure to provide an action plan), the DSC of establishment shall communicate to the Commission and the Board its opinion on whether the VLOP has terminated or remedied the infringement.

The Commission, in this phase, upon the Board's request or, of its own initiative after consulting the Board, in cases where an infringement has been found, shall take over the investigation.[34] The Commission may also act upon the request of the DSC of establishment [Article 46(2)] or if, after having enticed the DSC of establishment to act, pursuant to Article 45(7), the latter has not taken any investigatory or enforcement measures. To conduct its investigations and ensure compliance with the DSA, the Commission is granted a relatively wide array of powers. The Commission may ask the VLOP, or any person in the context of their professional activity that may reasonably be aware of information relating to the infringement, to provide such information. It may conduct interviews and take statements and require the VLOP to submit itself to an on-site inspection, during which the Commission may interview staff and key personnel of the platform and ask for information on the functioning of the latter's IT systems, algorithms, data handling, and business conducts. In urgent situations where there is serious risk of damage to the recipients of the service, for a specified period of time and on the basis of a *prima facie* finding of an infringement, the Commission may impose interim measures on the platform. The Commission is additionally entitled to take commitments from the VLOP and make them binding, declaring, in those cases, an end to the proceedings, with the possibility of reopening them whenever this decision is based on incomplete, incorrect or misleading elements, there is a material change in the facts, or if the VLOP's acts are contrary to the commitments it assumed (Article 56). Additionally, the Commission may monitor the effective implementation and compliance with this Regulation by VLOPs, namely by asking for access to, and explanations oF, their databases and algorithms.

When the proceedings result in a finding of non-compliance, either with the obligations held on the VLOP pursuant to Section 3 of Chapter 4, with any interim measure imposed by the Commission, or with a binding commitment assumed pursuant to Article 56, the Commission shall adopt a decision confirming the finding of non-compliance, communicating to the VLOP the measures that it considers taking or that it considers the VLOP should take. If the VLOP takes the necessary measures to address the Commission's findings, the latter shall close the investigation.

The aforementioned decision of non-compliance may be accompanied by the imposition of a fine not exceeding 6% of the VLOP's total turnover by reference to

[33] The Commission and the Board may, of their own initiative, request the DSC of establishment to investigate – the Board should also pass on this request whenever three DSCs of destination (DSCs of Member States where a platform offers its services) so request.

[34] At this stage, the DSC of establishment should communicate to the Commission all the elements it has on the suspected infringement or that may otherwise be relevant to the proceedings.

the preceding financial year (Article 59). In cases where the VLOP, intentionally or negligently, supplies incorrect, incomplete, or misleading information in response to a request for information, fails to rectify incorrect, misleading, or incomplete information upon request by the Commission, or refuses to submit to an on-site inspection, the Commission may impose an additional fine not exceeding 1% of the total turnover by reference to the preceding financial year. In any case, when fixing the amount of the fine, the Commission shall consider the nature, gravity, duration, and recurrence of the infringement or the delay caused to the proceedings. The Commission may, lastly, impose periodic penalty payments, not exceeding 5% of the average daily turnover by reference to the preceding financial year, on VLOPs or persons to whom information requests were sent, for their failure to comply with the measures ordered in the course of the investigation (Article 60). The exercise of the powers granted by Articles 59 and 60 shall be subject to a limitation period of five years, to be counted from the day in which the infringement is committed or, in the case of continuing or repeated infringements, from the date in which the infringement ceases (Article 61). The enforcement of the penalties imposed in the context of the exercise of the powers referred to in Articles 59 and 60 is also subject to a limitation period of five years (Article 62). All the decisions of imposition of fines or penalty payments, as well as findings of non-compliance, interim measures, and binding commitments must be published.

Should all measures highlighted over the course of this section fail, the Commission, in the face of a persisting infringement which causes serious harm which cannot be avoided by any other means, after granting two weeks for the submission of written observations by all interested parties, shall ask the DSC of establishment to request from a national judicial authority the temporary restriction of access to the recipient of the service concerned with the infringement or, if not technically possible, to the online interface of the VLOP, pursuant to Article 43(3). We should note here that, in this particular case (Article 65), there seems to be no requirement that the infringement entails a serious criminal offense involving the threat to the life or safety or persons for the DSC of establishment to make use of this power. This gives a stronger rational to the two-week period for the submission of written observations by interested parties (see, on the contrary, section 5, regarding the DSCs powers in this regard).

7. Final comments

The DSA is intended to be the cornerstone of the Digital Single Market, restructuring the current framework so that it is adequate for the present necessities and adaptable to future innovations. If we consider the fact that the present Regulation is looking to govern technologies (and issues caused by their introduction to the markets) that are still at early stages of development or have yet to be developed, we can understand the intended broadness in language and in rules. Notwithstanding that, we cannot afford to waste the opportunity to make the necessary changes to effectively address present issues, especially considering that we might have to work within the framework put in place for the next 20 years, as was the case with the E-Commerce Directive. The DSA puts forward proposals that at first sight might seem groundbreaking – when compared to the current functioning of the market – but, upon further consideration, do not address the imbalance of power between platforms and their users, the necessary differentiation between platforms, or ensure the highest possible level of protection

of fundamental rights. In these final comments, we will strive to highlight some areas where the legislators have room to improve the Commission's proposal.

While the proposal clearly focuses on imposing a strong transparency and accountability regime for providers of intermediary services, specifically online platforms, the actual provisions give the users' very little additional control over the interactions they have with the platforms, and, generally, are contingent to an action on their side as opposed to being set by default. If we consider the regime on online advertisement, the main novelty is the increased transparency on the parameters used to determine the target audience of a specific ad, as well as the person or entity on whose behalf the ad was bought. While this is clearly a welcome, initiative it is still a long way from giving users actual control over the advertisements that they see or even to ensure that all their online activity is not being tracked for this purpose. As the proposal stands, it completely sidesteps the requests made by the European Parliament (and supported by the EDPS) for a distinct regime for ads based on pervasive tracking and ads not based on pervasive tracking, with the intent to implement a phase-out regime leading to a prohibition of the former.[35] This is further compounded by the fact that, as regards VLOPs, the only additional requirements are the maintenance of a database containing this information, without any due regard being paid to the difference in risk between them and emerging online platforms. The latter, being of a smaller size, benefiting from less access to data and, hence, posing a reduced threat by comparison, could potentially have retained greater access to the use of targeted advertising, while VLOPs saw their options in this regard reduced. This is particularly important due to their role in allowing for single sign in to many platforms, allowing them to track user activity even across third party websites. The only escape valve in this context would be if we considered that, as regards, VLOPs, ads are to be considered "*information*" for the purpose of content moderation (something which is not clearly stated in Article 29 but does not seem incompatible with the definitions contained in Article 2), though, even there, the proposal still requires that users opt out of the recommender systems based on profiling, as opposed to the default being an option not based on profiling – a route which the EDPS supports.[36]

As regards terms and conditions, the proposal does little to make them more accessible to the public, missing the opportunity to impose a stricter duty to inform users on their main aspects in a separate and reduced format with less technical language. The proposal also does not go into the details of what should be considered illegal content making a general reference to EU and national law, with occasional exceptions, meriting the EDPS's criticism.[37] Though it would prove impossible and counterproductive to aim for an exhaustive list of the applicable legislation, a wider array of examples would prove useful to the providers, as the nature of the activity and type of illegal content that intermediary service providers must consider varies widely from sector to sector. We also note that, as regards the right to lodge a complaint (Article 43), the DSCs are not obliged to provide feedback to the persons that lodged the complaint. While national administrative law might safeguard the right to such feedback, there is room to harmonise this right across the EU.

[35] European Parliament, Resolution on the Digital Services Act and fundamental rights issues posed (2020/2022(INI)), paragraph 17, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0274_EN.html and EDPS, Opinion 1/2021, paragraph 69.
[36] EDPS, Opinion1/2021, paragraph 14.
[37] EDPS, Opinion1/2021, paragraph 27.

A note should also be made to address two issues raised by the European Parliament that are of particular importance and were not contemplated on the proposal: (i) those of interoperability of VLOPs with, for instance, software that allows for users to customise privacy and content curation preferences across multiple platforms,[38] and the increasingly pressing issue of personalised pricing,[39] which finds no mention in the proposal.

As a final consideration, we should make reference to Section 5 of Chapter III which governs the Commission's and the Board's involvement in the drafting of standards, codes of conduct, and crisis protocols, leading us to believe that this is yet another area where soft law will be prolific and influential (it should be noted that while adherence to codes of conduct is voluntary, Recital 68 determines that an unjustified refusal to adhere to one, upon the Commission's invitation, might be taken into consideration when determining if the online platform infringed its obligations under the DSA). A combination of soft and hard law might, indeed, be the only possible route to tackle the issues posed by the new online environment, in a manner that ensures the protection of fundamental rights, namely freedom of expression and information (especially susceptible to interference by public and private actors). The Commission intends to anticipate some of the rules laid out in the DSA through the revision of the Code of Practice on Disinformation, having suggested to the signatories, in a recently issued guidance, the inclusion of many equivalent provisions in the revised Code.[40] So far, the Commission has not made public whether the signatories have already presented a draft for the revision, but anticipating these measures through the Code would be an opportunity to test the effectiveness of the measures and would serve to breach the gap while the final text of the DSA is not approved.

[38] European Parliament, Resolution (2020/2019(INL)), paragraph 22.
[39] European Parliament, Resolution (2020/2018(INL)), paragraph 32.
[40] European Commission, Guidance to strengthen the Code of Practice on Disinformation (COM(2021) 262 final), *https://ec.europa.eu/newsroom/dae/redirection/document/76495*.