THE DIGITAL SERVICES ACT – A LAUDABLE AMBITION, BUT WILL IT DELIVER?

BY
MICHÈLE LEDGER

&
LAURA SBOARINA

Respectively, Head of Practice - Cullen International, Researcher and Lecturer at CRIDS/NADI - University of Namur, Research Fellow – CERRE; and Principal Analyst - Cullen International.

Visit **www.competitionpolicyinternational.com** for access to these articles and more!

THE DIGITAL SERVICES ACT – A LAUDABLE AMBITION, BUT WILL IT DELIVER?

By Michèle Ledger & Laura Sboarina

The EU has adopted the Digital Services Act ("DSA") a ground-breaking legislation to make the internet a safer place, while also seeking to protect fundamental rights and to enhance consumer protection. This horizontal framework places important responsibilities on intermediary services, depending on their reach and size relating to the moderation of content. Other – more surprising aspects – are also covered such as online advertising and dark patterns, while the moderation of media services is not addressed (but is now covered in the Commission's European Media Freedom Act). The DSA places a large emphasis on oversight and enforcement but will the DSA deliver or is it too ambitious?

01
INTRODUCTION

The Regulation on a Single Market for Digital Services and amending Directive 2000/31/EC, nicknamed the Digital Services Act ("DSA") was finally adopted on 4 October 2022, less than two years after it was first proposed by the European Commission. It was published in the Official Journal on October 27, 2022 and while some of its provisions will apply earlier, it will be directly applicable in the 27 Member States on February 17, 2024.[2]

The DSA is a horizontal instrument introducing different tiers of obligations to be applied by online intermediaries (depending on their reach) to counter the dissemination of illegal and harmful content while also seeking to protect freedom of expression. At the same time, the DSA also introduces rules to protect users against misleading online advertising, recommender systems and so-called dark patterns. It carries over the rules on the liability of intermediaries that are contained in the Electronic Commerce Directive[3] without changing these rules very substantially.

This article explores some of the most striking aspects of the new regulation, linked to the fact primarily that the DSA is a horizontal legal framework. It focuses on its (very broad) scope, the obligations to deal with illegal and harmful content, the safeguards against arbitrary content moderation (including of media services), and some of the enforcement and oversight aspects of the new regulation.

02
SERVICES IN SCOPE

The DSA applies to an extraordinary wide range of online services.[4] These are intermediary services defined[5] as a sub-set of information society services[6] i.e. mere conduit, caching and hosting services which were hitherto also defined and regulated under the Electronic Commerce Directive.[7] The DSA in fact repeals the references in the Electronic Commerce Directive to these services and to the rules on liability for third party illegal content and re-introduces them (with some clarifications) in the DSA.

Mere conduit and caching services are the technical internet layer and cover services such as internet access services, electronic transmission services and proxy servers.[8]

It is quite surprising that these services are covered because none of the other legal instruments that have introduced responsibilities on online intermediaries have so far targeted the technical layer. It would seem that these intermediaries are covered primarily because the DSA is now the home of the rules on the liability of intermediaries which also cover these technical intermediaries. This may create a number of difficulties since these intermediaries are also regulated under the European Electronic Communications Code[9] and are hence under the oversight of the national regulatory authorities ("NRAs") in charge of electronic communications services, whereas the DSA introduces a new layer of supervision of these intermediary services as explained below.

2 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065&from=EN.

3 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 ((OJ L 178, 17.7.2000, p. 1).

4 M. LEDGER, S. BROUGHTON MICOVA, Overlaps - services and harms in scope : comparison between recent initiatives targeting digital services, Bruxelles, CERRE, 2022, 52 p.

5 Article 3 (g) of the DSA.

6 Information society services are defined in Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

7 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 ((OJ L 178, 17.7.2000, p. 1).

8 Schwemer, S., Mahler, T. & Styri, H. (2020). Legal analysis of the intermediary service providers of non-hosting nature. Final report prepared for European Commission.

9 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

Hosting services cover for instance (on top of online platforms defined as explained below) cloud computing and webhosting services.

The DSA places more responsibilities on online platforms – a subcategory of hosting services – that at the request of a recipient of the service, store and disseminate information to the public (a potentially unlimited number of third parties) unless that activity is a minor or purely ancillary feature of another service.[10] This is potentially the largest category since it covers social media platforms, video-sharing services, app stores, marketplaces but also the travel, transport and accommodation services platforms to the extent of course that they qualify as information society services.[11] Further obligations are also placed on online marketplaces and other platforms that allow consumers to conclude distance contracts with traders. [12]

Despite not having been initially specifically covered by the proposal, online search engines are now clearly in scope. They are defined as a special type of intermediary service[13] but except for paid for (or sponsored) search results, which are – in line with the case law of the Court of Justice of the EU – considered as hosting services, it is not clear if natural or organic search results will be categorised as caching or hosting services. This may have legal consequences as the duties for caching and hosting services are not identical.

Then the largest responsibilities are placed on the very large online platforms ("VLOPS") and search engines ("VLOSES").[14] These are the platforms or search engines that have at least 45m active recipients in the EU on a monthly basis. This represents around 10 percent of the EU's population. The VLOPS and VLOSES will be designated by the Commission and their names will be published in the Official Journal.

Lastly, like many of the more recent EU legislations, intermediaries that do not have an establishment in the EU will be covered if they have a substantial connection with the EU. This could be deemed to exist if they have a significant number of recipients in one or more Member States in relation to the population, or if the service provider targets its activities towards one or more Member States as evidence by relevant circumstances such as language or currency. [15]
The DSA also foresees waivers from certain of the obligations for micro and small enterprises.

This extremely wide scope of application may cause practical difficulties. Indeed, no mechanism is foreseen in practice on the designation process of the intermediaries in scope, except as explained above for the VLOPS and VLOSES which will need to be designated by the European Commission. Some Member States may therefore launch studies to understand which services they will need to regulate, while others may want to introduce a self-declaration or notification requirement of the intermediaries established in their countries.

03
HARMS IN SCOPE

The DSA also has an extraordinary wide scope of application in terms of the harms in scope. It deals primarily with countering the dissemination of illegal content, which is defined in a very broad manner.[16] First, it covers information irrespective of its form: content, products, services or activities are all in scope. Then, illegality is defined by reference to what is not in compliance with Union law, or the law of any Member State, provided that national law is in compliance with Union law, irrespective of the precise subject matter or nature of the law.

It is therefore striking to note that, except for some caveats explained below, all breaches of law are treated in the same manner. A breach of consumer protection legislation will be treated in the same manner as a conduct that constitutes a criminal offence. This may lead platforms to be flooded with requests to remove content considered to be illegal on "trivial grounds," leading perhaps to delays in the

10 Article 3 (i) of the DSA.

11 See in particular Case C390/18 *Airbnb Ireland UC v. Hotelière Turenne SAS,* [2019], Case C- 434/15 *Elite Taxi v. Uber Systems Spain SL,* [2017], Case C62/19 *Star Taxi App SRL v. Unitatea Administrativ Teritorială Municipiul Bucureşti prin Primar General and Consiliul General al Municipiului Bucureşti,* [2020].

12 These rules are detailed in Section 4 of the DSA.

13 Article 3 (j) of DSA.

14 These rules are detailed in Section 5 of the DSA.

15 Article 3 (d) (e) of the DSA.

16 Article 3 (h) of the DSA.

processing of the serious requests. We note for instance that the UK's Online Safety Bill[17] which is being discussed in the UK Parliament introduces a tiered approach, since it lists "priority offences" which platforms need to remove with priority.

The second element that appears surprising is that there is no real mechanism to help intermediaries determine if the national legislation that is alleged to be breached is in line with Union law, which includes of course the EU Charter on fundamental rights. Does the platform need ipso facto to examine this (in)compatibility or does the (in)compatibility need to be raised by the person's whose[18] content could be removed? In addition, deciding on the (in)compatibility may require a complex legal analysis, which may not be able to be carried out by the platform itself.

That being said, it may also be noted that the DSA also covers the category of "manifestly illegal content" but only defines this category, by saying that this is where it is evident to a layperson, without any substantive analysis that the content is illegal.[19] In relation to this type of content, as explained below, online platforms are required to suspend accounts in relation to users that frequently post such content. It also obliges hosting services to notify to law enforcement or judicial authorities any suspicions that a criminal offence, involving a threat to life or safety has oris taking place or is likely to take place.[20]

Harmful content is dealt with in the DSA but in an indirect manner as explained below. In any event, the co-legislators have been careful not to define this notion, unlike in the UK's Online Safety Bill.

It must be noted that more focussed legislation exists in the EU to either set more detailed obligations in relation to certain specific harms such as terrorist content[21] or in relation to specific types of online intermediaries such as video-sharing platforms,[22] or both. For instance, the Directive on Copyright and the Digital Single Market deals with online content sharing platforms and their duties in relation to the clearance of copyright uploaded by the users of the platforms.[23] Legislation to tackle the dissemination of child sexual abuse and grooming is also in the process of adoption.[24]

04

OBLIGATIONS TO DEAL WITH ILLEGAL CONTENT

The DSA does not introduce a requirement for platforms to filter illegal content before it is uploaded by their users as this would disproportionately limit users' freedom of expression and freedom to receive information.[25] Instead, it requires all platforms (except the technical internet intermediaries) to operate a notice-and-action procedure whereby platforms must deal with illegal content when users send notifications and (depending on the type of platform) take additional measures for content that is "manifestly illegal." Also, VLOPS and VLOSEs must conduct an annual risk assessment of how their service contributes to the dissemination of illegal content and take the appropriate measures of their choice to mitigate the risks identified. Additional specific provisions apply to online marketplaces with the purpose of fighting fraudulent practices and the sale of illegal products.

The notice-and-action procedure must comply with a set of obligations. The most interesting one is that the DSA speci-

17 https://bills.parliament.uk/bills/3137.

18 https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html.

19 Recital 63 of the DSA.

20 Article 18 of the DSA.

21 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of the terrorist content online (OJ L 172, 17.5.2021, p. 79)

22 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 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) (OJ L 95, 15.4.2010, p. 1).

23 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 (OJ L 130, 17.5.2019, p. 92).

24 Proposal for regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, 2022:0155(COD), 11.5.2022, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN.

25 Article 8 of the DSA prohibits member states (as in Art. 15 the 2000/31/EC E-Commerce Directive, now deleted) to impose a general obligation on information society services to monitor the information or to actively seek illegal information.

fies the elements that need to be contained in the notices (e.g. exact location and grounds for considering the content illegal.)[26]

It must be noted that when the notice is accurate, the platform will be presumed to have actual knowledge and could therefore risk incurring liability but only where a diligent provider would be able to determine the illegality of the notified content "without a detailed legal examination." Fundamental rights associations have welcomed this clarification introduced by co-legislators because otherwise platforms would be "inappropriately required to make determinations on the illegality of content" and incentivised to "remove any content notified to them," beyond content that is "evidently manifestly illegal." [27]

Platforms are required to process (including automatically) any notice they receive through this system, and to take "timely" decisions about it. However, online platforms (i.e. not the technical hosting services) must immediately act (or decide not to act) when they receive notices from so-called "trusted flaggers."[28] These are (public or non-governmental) entities with proven expertise and independence from platforms that will be designated by the relevant Digital Service Coordinator ("DSC") that will need to be designated by the Member States as explained below.

In all cases, platforms must inform flaggers of the decision taken and of the possibility to complain. To avoid misuses, the regulation requires online platforms to suspend users that frequently submit manifestly unfounded notices.

As mentioned above, platforms must take further measures to deal with content that is manifestly illegal (e.g. criminal offences). In particular, all platforms (including technical hosting service providers) need to immediately report to the relevant law enforcement or judicial authority any suspicion of a criminal offence that has or is threatening someone's life or safety (or is likely to do so), such as child sexual abuse.[29]

Online platforms must also temporarily suspend the service for users that frequently provide any content that is manifestly illegal (irrespective of how they get aware of it).[30]Interestingly, the DSA does not provide any details as to the meaning of what constitutes a frequent infringement or the length of the required suspension. However, it specifically requires online platforms to specify in T&Cs their policies regarding frequent infringers with examples of conducts and length of suspensions. In any event, before suspending the provision of the service, they would need to send a prior and detailed warnings to the users concerned.[31]

The regulation accurately details how the VLOPS and VLOSES must undertake the annual assessment of the risk of dissemination of illegal content but interestingly it does not provide criteria to define when the results of the assessment require action.[32] Also, the choice of the specific measure remains with the provider. Only a recital clarifies that the relevant risk might be identified when access to illegal content spreads rapidly and widely through accounts with a particular wide reach or other means of amplification.[33] One of the mitigation measures mentioned in the DSA that seems relevant in this regard is adapting the speed and quality of processing notices related to specific types of illegal content.

That said, the Commission can adopt guidelines to present best practices and recommend possible measures.

05

OBLIGATIONS TO DEAL WITH HARMFUL CONTENT

On top of rules to fight the dissemination of illegal content, the regulation includes some provisions to address content that is harmful but not necessarily illegal, such as disinformation or content that is harmful to minors.

26 Art. 16 of the DSA.

27 Centre for Democracy and Technology "A series on the EU Digital services Act"

28 Art.22 of the DSA.

29 Art.18 of the DSA.

30 Art.23 of the DSA.

31 Article 24.4 of the DSA.

32 Arts 34 and 35 of the DSA.

33 Recital 80 of the DSA.

Under the regulation, platforms that are accessible to minors (for instance if the T&Cs allow users under the age of 18) must take appropriate measures to ensure a "high level of protection of safety, security and privacy of minors"[34]. Rules are not further detailed. The recitals explain that this could be ensured for instance by "adjusting the default settings of the service interface"[35] since "the design of the interface could intentionally or unintentionally exploit the weaknesses and inexperience of minors."[36]

"Actual or foreseeable negative effects on the protection of minors" are also included within the list of systemic risks that VLOPs and VLOSEs must assess. Examples of mitigation measures (against the risk of exposure of minors to harmful content) include age verification and parental control.

Another important category of systemic risks addressed by the regulation is the dissemination of disinformation. Article 34 mentions "negative effects on civic discourse and electoral processes, and public security" or "on the protection of public health." Examples of mitigation measures include the "prominent marking" and a flagging system for deep fakes, discontinuing advertising revenue for specific information (or improving the visibility of authoritative information), and participating in codes of conducts.

It is interesting to see that if the EU faces a serious crisis (e.g. a pandemic or a war), endangering public health or security, the European Commission is empowered to require one or more VLOP or VLOSE to conduct a specific risk assessment and take specific mitigation measures.[37] Fundamental rights associations[38] criticise the excessive interference of the Commission, which can not only engage in a dialogue with providers to identify specific mitigation measures but also review them if the reported results are considered insufficient. The regulation establishes that these measures can be taken for maximum three months. However, this period can be extended. In addition, the Commission must encourage platforms to participate in the application of crisis protocols and for instance prominently display information on the crisis that is provided by the EU or member states. Also outside of a crisis, the Commission can invite relevant providers to participate in EU codes of conducts.

In the case of disinformation, the powers of the European Commission to direct how platforms address content during a crisis is considered particularly problematic because of the potential consequences on freedom of expression and citizen's rights to be informed.[39]

Also, content moderation polices regarding disinformation that are implemented by platforms are often contested. One emblematic case is the ban from YouTube (overturned afterwards) of a national UK radio, TalkRadio, for COVID-19 content that explicitly contradict expert consensus.[40]

06

SAFEGUARDS AGAINST ARBITRARY CONTENT MODERATION AND THE CASE OF MEDIA SERVICES

To protect users against arbitrary or erroneous moderation of their content, the regulation requires all platforms (including technical hosting service providers) to adequately inform users in a timely manner every time they act against their content.[41] Also, online platforms need to give users the possibility to complain through an internal complaint-handling system that must have certain characteristics.[42]

Interestingly, platforms must do so not only when they remove content or suspend users accounts but also when they

34 Article 28 of the DSA.

35 Recital 71 of the DSA.

36 Recital 81 of the DSA.

37 Arts.37 and 48 of the DSA.

38 Centre for Democracy and Technology "A series on the EU Digital services Act"

39 Will the Digital Services Act save Europe from disinformation? Centre for European Reform

40 BBC TalkRadio: YouTube reverses decision to ban channel.

41 Art.17 of the DSA

42 Art. 20 of the DSA.

restrict at any degree the availability, visibility or monetization of content (e.g. when the ranking of content is decreased).

Further, online platforms must fairly process with a qualified staff (and not only by automated means) all the complaints they receive through the internal complaint-handling system and, where relevant, they must swiftly reinstate the disputed content or provide information about other redress possibilities.

Users are always entitled to refer the matter to courts but the regulation also allows them to seek a faster resolution (maximum 6 months) by referring the dispute to independent alternative dispute resolution entities that will need to be certified as such by the DSCs. These bodies do not have the power to impose binding decision to settle the dispute but the regulation obliges online platforms to engage in good faith with them.[43]

The regulation requires all intermediaries to inform users (in their T&Cs) of any restriction to the use of the service and to apply T&Cs fairly.[44] As far as restrictions are listed in T&Cs, it would seem that these providers remain free to restrict the use of the service beyond content that is illegal or harmful as defined in the DSA.

Users of platforms and search engines include media services and, as pointed out by the EU media associations, citizens increasingly access editorial media content (press, audiovisual, radio) online through the services of these providers.[45] The restriction of lawful content by media services on a social media, as well as the delisting of a whole media service from an app store or its down-ranking on a search engine, for its incompatibility with the service T&Cs, can have a great impact on citizen's freedom to receive information.

To protect media services (that are under the editorial responsibility of a regulated provider) from the interference of platforms, some members of the European Parliament had proposed the introduction of a media exemption,[46] which was however rejected.

Instead, with the same purpose but in a weaker way, the regulation requires platforms to consider freedom and pluralism of the media when applying their T&Cs.[47] Further, the regulation requires VLOPs and VLOSEs to include in their risk assessment the impact of the service on the exercise of fundamental rights, including "freedom of expression and of information" and "media freedom and pluralism," and take the appropriate mitigation measures.

Interestingly, following the adoption of the DSA, the European Commission decided to include some additional obligations for VLOPs regarding the moderation of regulated media services in a separate (sector-specific) legislative instrument that would apply on top of the regulation. The proposal for an EU Media Freedom Act ("EMFA") was adopted on 16 September 2022[48] and was at the time of writing, under scrutiny by co-legislators.

> ***The regulation requires all intermediaries to inform users (in their T&Cs) of any restriction to the use of the service and to apply T&Cs fairly***

The proposed obligations would apply to VLOPS as defined in the DSA but not to VLOSES and only in favour of media outlets that have self-declared to the platform (which is bound to provide the related functionality) that they are regulated in the EU as media services (including by widely recognised self or co-regulatory standards), and that they are independent from member states and third countries. It would seem therefore that it would be up to VLOPs (with the help of Commission's guidelines) to determine whether a media outlet fits with the criteria and that media outlets without an establishment in the EU would not be able to benefit from this media exemption.

43 Art.21 of the DSA.

44 Art.14 of the DSA.

45 Joint statement by EU media association on the DSA trilogue.

46 On 14 Dec. 2021 the lead Consumer Protection and Internal Market (IMCO) Committee of the European Parliament rejected both Amendment 79 (new art.7a) of Opinion of Culture and Education committee and Amendment 281 (art.27anew) of Opinion of the Legal Affairs committee which were introducing the prohibition to interfere with, remove and suspend accounts of editorial content services that are published in compliance with the law.

47 "Diligent, objective and proportionate" (art.14).

48 Proposal for a regulation establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU.

In particular, VLOPS would be required to process complaints received by these media services (against any moderation of their content, on any ground) through a fast-track procedure.[49] Also, when they restrict content ("suspend the provision of the service in relation to that content") on T&Cs grounds, they would have to "take all possible measures" to provide a statement of reasons before their action takes effect (rather than in a timely manner), unless the content contributes to one of the systemic risks identified by the DSA (e.g. disinformation).

It is interesting to note that these obligations would not cover journalistic content that is provided outside of the editorial responsibility of a media (e.g. from citizen journalists). Also, contrary to similar provisions under discussion in the UK,[50] the proposal does not oblige the platform to refrain from taking action against the content while it reviews a complaint.

Finally, VLOPS would have to effectively engage in good faith in a dialogue "to find an amicable solution" with any of these media that requests it and that consider that the provider frequently restricts or suspends its content without sufficient grounds. They would also need to publish annual information on restrictions or suspensions of (regulated) media services on incompatibility grounds with the service's T&Cs. Information must include the number of instances and the grounds.

The European association of press publishers has criticised the proposal because it subjects the press to the interference of "not only platforms but also media regulators" to the detriment of press freedom.

According to the association, these "weak procedural safeguards do not remedy but rather further enshrines the right given by the DSA to large online platforms to censor legal editorial content on the basis of their terms and conditions."[51]

07
OTHER AREAS

The wide scope of the DSA is yet again apparent as it also deals with other aspects: online advertising,[52] recommender systems[53] and dark patterns.[54] In our view, these aspects do not fit comfortably in the DSA. While these are important provisions, it would have probably been best to address these areas in more horizontal pieces of legislation since there is no reason why they should be limited to intermediaries.

In a nutshell, the DSA aims to ensure that users are not forced into making a decision (e.g. giving their consent), can identify in real time each advert as such (including who paid for it) and are informed of the parameters used to target advertising to them and on how to change them. Users cannot be targeted with advertising on the basis of sensitive personal data (e.g. political opinion or sex orientation) or if they are minors. Users of VLOPs and VLOSEs must have access to an advertising repository. Platforms must also inform users in T&Cs on how their recommend content to users, and of options to modify the underlying parameters.

VLOPs must also provide one recommender system that is not based on profiling.

Indeed; all online websites, including editorial curated services, should avoid dark patterns and be subject to rules to protect users against online advertising and recommender systems.

A. Oversight and Enforcement

The DSA places a very large emphasis on the oversight and enforcement of the rules it introduces. [55] For all platforms, except for the obligations that only apply to VLOPS and VLOSEs, the member state where the intermediary is mainly established has the exclusive power of supervision and enforcement of the DSA, through national competent authorities. One of these authorities will need to be designated as a DSC by February 17, 2024.

49 Art.17 of the proposed EMFA.

50 UK government amendments on journalistic exception Online Safety Bill (section 16 Duties to Protect Journalistic Content).

51 ENPA statement of Sep. 2022.

52 Articles 26 and 39 of the DSA.

53 Articles 27 and 38 of the DSA.

54 Article 25 of the DSA.

55 Chapter 4 of the DSA.

This is a stark contrast, compared to the previous situation, where most of the services were not under the scrutiny of a sector specific national regulator. Some services (electronic communications services and video-sharing platforms in particular) are however already under the oversight of a sector specific regulator.

DSCs will be responsible for all matters relating to enforcement and supervision unless a member state decides to assign certain specific tasks or sectors to other competent authorities.[56] In all cases the respective tasks and competences of all authorities and the DSCs will need to be clearly defined and the names and tasks communicated to the European Commission and the to the newly created European Board for Digital Services.[57] At the time of writing, the member states were in the process of working out their institutional arrangements with various solutions envisaged, ranging from awarding the DSC status to the media regulatory authority, the competition authority, the electronic communications authority or to a newly created authority (other solutions are also envisaged). These institutional arrangements are far from simple because as explained above, the DSA covers many types of intermediaries and because many areas are covered, which means that multiple authorities may be well placed to supervise the application of the rules.

B. VLOPS and VLOSES to be overseen by the European Commission

After a lot of discussions, the European Commission was given the exclusive power to oversee the additional obligations that are incumbent on the VLOPS and VLOSES (or if they have systematically infringed the other provisions of the regulation).[58] To cover the costs of supervision, the DSA foresees that these operators will need to pay an annual supervision fee to the Commission, which will be determined by the Commission through the adoption of a delegated act, and which will take into account the costs incurred in the previous year while being proportionate to the number of monthly recipients of the platforms. In any case, the fee will not be able to exceed 0.05 percent of the platform's worldwide annual net turnover of the preceding year. Nothing is foreseen on the supervision fees that may (or not) be levied at the national level, whereas the DSA foresees that the authorities in charge should be independent and sufficiently funded.[59]

> ***DSCs will be responsible for all matters relating to enforcement and supervision unless a member state decides to assign certain specific tasks or sectors to other competent authorities***

Also, to facilitate the oversight of the large platforms, other measures are introduced. First, just like in the financial sector, independent auditors will need to assess whether they comply with their due diligence obligations as well as the commitments they make through code of conduct and crisis protocols. In case of a negative audit report, the VOPS and VLOSES will need to publish an audit implementation report explaining how they intend to remedy the situation.[60] Second, like in the GDPR,[61] a compliance function is foreseen whereby compliance officer(s) are responsible for cooperation with the DSCs and the European Commission and who will be responsible for informing and advising the management and staff about the obligations of the DSA. Then, very interesting mechanisms are foreseen on giving access to vetted researchers (and to the DSCs and the European Commission) to data held by VLOPS and VLOSEs to help them conduct research on systemic risks and risk mitigation measures.[62] Among the many investigation powers that are given to DSCs and the Commission, we also flag the fact that VLOPS and VLOSEs can be ordered by the Commission to provide them access to their algorithms.[63]

56 Article 49 of the DSA.

57 Article 61 of the DSA.

58 Article 65 of the DSA.

59 Article 43 of the DSA.

60 Article 37 of the DSA.

61 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

62 Article 40 of the DSA.

63 Article 72 of the DSA.

VLOPS and VLOSEs could be fined up to 6 percent of their total annual word turnover if they are found to be in breach of the regulation.[64]

08
CONCLUSIONS

In short, on paper the DSA is certainly what it set out to be: a horizontal EU wide regulation covering intermediary services by establishing specific due diligence obligations tailored to specific categories of providers of services.

In practice however, it may be difficult to put into application.

First because it covers a very wide range of service providers, including the technical internet intermediaries. More fundamentally the scope of the illegal harms seems particularly wide. All types of illegal content are treated in the same way except for certain caveats, which could mean that platforms could be flooded with requests to take down content. There are no mechanisms to help the platform to determine if the national law that could be breached is in line with EU legislation, which may also cause problems for them.

Platforms are obliged to include in their T&Cs their content moderation policies and to supplement some of the rules of the DSA, and in particular those on the suspension of users and on the risk mitigation measures to be taken. However, it is our understanding that platforms remain free to restrict the use of the service beyond content that is illegal or harmful as defined in the DSA.

Therefore, although it is laudable that users are informed of and entitled to complain against all moderation decisions (including down-ranking or demotions), platforms may once more be flooded with requests, in particular because complaints must be subject to human review. In practice, and if online platforms encounter such difficulties, the rights of users will ultimately be undermined. It is true however that users can always refer the matter to alternative dispute resolution bodies but platforms (and users) could potentially refuse to accept their decisions, since the DSA foresees that their decisions are not binding.

Regretfully the DSA did not specifically address the issue of the moderation of media outlets by the larger platforms and even before the DSA was adopted, the Commission had already proposed rules to protect the integrity of media services on VLOPs in another legal instrument, the EMFA.

The obligation to conduct a risk assessment (and eventually take mitigation measures) on the impact of the service on freedom of expression, and freedom and pluralism of the media, is extremely wide and could also be difficult to deliver in practice.

This broad scope of application is also reflected in added areas that are addressed in the DSA, namely the rules on dark patterns, recommender systems and online advertising, which in our view do not comfortably sit in the DSA.

The European Commission has a fundamental role to play in the follow-up to the DSA. First it will be the sole enforcer of the added rules that apply to VLOPS and VLOSES, although many new mechanisms are foreseen such as independent auditors, the compliance function and the possibility for vetted researchers to get access to data belonging to VLOPS and VLOSEs. Also, it will be allowed in case of crisis to directly interfere with the choice of measures including to address disinformation.

Lastly, the Commission has the power to adopt guidelines, delegated and implementing acts, and to promote voluntary standards. In some areas, it will be particularly interesting to see to what extent the Commission will use these powers, which no doubt will help to shed more light on some of the concepts of the DSA.
In terms of enforcement, more generally, the DSA marks a shift in approach and places a lot of responsibility on national DSCs, which will need to be designated by 17 February 2024.

It remains to be seen however if these national authorities and the European Commission will be sufficiently well funded and equipped to carry out in a proper way their supervision and enforcement tasks under the DSA.

> ***The European Commission has a fundamental role to play in the follow-up to the DSA***

64 Article 74 of the DSA.

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL