Instituut voor Informatierecht
Institute for Information Law

Digital Services Act (DSA) Observatory

Institute for Information Law (IViR), University of Amsterdam

Discussion paper - version of 28 October 2021

"The Digital Services Act (DSA) proposal: a critical overview"

Ilaria Buri

Joris van Hoboken

Published as part of the DSA Observatory, a research project by the Institute for Information Law (IViR) at the Faculty of Law University of Amsterdam, with the support of Open Society Foundations.

Table of Contents

Introduction

This discussion paper sets out to provide a critical overview of the context and substantive provisions of the Digital Services Act ("DSA") draft regulation presented by the European Commission in December 2020.

This paper is comprised of two parts. Part I provides an overview of the broader legal and policy context of the DSA package, briefly illustrating the existing EU legal framework for digital services and some of the initiatives undertaken in recent years in this domain.
Following the structure of the DSA proposal, Part II of the paper provides an illustration of the rules introduced by the DSA proposal, covering the articles under Chapter I ("General provisions"), Chapter II ("Liability of providers of intermediary services") and Chapter III DSA ("Due diligence obligations for a transparent and safe online environment"). Chapter IV DSA on implementation, cooperation, sanctions and enforcement is not covered in this paper and will be discussed in further analysis.

The description of the relevant provisions includes reference to some of the positions expressed by various stakeholders in reaction to the DSA proposal. The paper also gives account of recent parliamentary developments in the DSA process, identifying some of the most significant amendments (and potentially contentious issues) in the DSA draft report of the lead IMCO Committee from May 2021 as well as in the opinions published by the LIBE and JURI Committees respectively in July and October 2021. The discussion highlights aspects of the proposal where clarifications, review and further debate are needed.

As the DSA legislative process continues, new and updated versions of this paper will be made available, to discuss legislative progresses in the European Parliament and the Council and other relevant developments in platform regulation.

1. The Digital Service Act proposal – the broader legal and policy context

1.1. Introduction

On 15 December 2020 the European Commission presented a draft Regulation on Digital Services, the "Digital Services Act" ("DSA")[1] and a draft Regulation on contestable and fair markets in digital sectors, the "Digital Markets Act" ("DMA").[2]

The background to these proposals can be found in the Communication "Shaping Europe's Digital Future"[3] of February 2020, when the European Commission announced the presentation of a comprehensive "Digital Services Act" rules package by the end of 2020. With the announced proposal the Commission set out to update and harmonize the rules applicable to providers of digital services, which are still mainly defined by the e-Commerce Directive from the year 2000[4], and to increase regulatory oversight over (dominant) online platforms in particular. Furthermore, in the context of the same package, the Commission would also consider *ex ante* rules to ensure the fairness and contestability of the markets domainated by large online platforms acting as gatekeepers. The DSA and the DMA proposals presented in mid-December 2020 reflect these two policy objectives.

The DSA proposal follows an evaluation of the e-Commerce directive, including a consultation with stakeholders and builds on the guidelines of the European Commission from the last years. The DSA proposal puts forward a horizontal legal framework applicable to all providers of intermediary services and dictates rules on the conditional exemption from liability of intermediaries, on asymmetrical due diligence obligations for a more transparent and safer online environment and on the implementation and enforcement of the new Regulation.
This first part of the discussion paper provides an overview of the broader legal and policy context in which the DSA package is situated and of the developments that led to the adoption of the proposal. While the specific (substantive) provisions of the DSA are described in Part II, the following paragraphs briefly illustrate the existing EU legal framework for digital services, including some of the initiatives undertaken more recently to address the challenges associated with the massive digitalization and platformization of the economy and society.

1.2. From the e-Commerce Directive towards a new legal framework for digital services and online platforms

[1] 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.
[2] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act).
[3] European Commission, Shaping Europe's Digital Future, COM (2020).
[4] 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 ('e-Commerce Directive')

1.2.1. The e-Commerce Directive and the evolution of the digital services ecosystem over the past two decades

The foundations of the existing EU legal framework for digital services were laid down by the e-commerce Directive, which introduced the core principles applicable to the provision of information society services[5] and introduced EU level conditional limitations for the liability of intermediary services for third party content. While the e-Commerce directive is still the cornerstone of the rules governing digital services in the internal market, the scale and impact of such services - from an economic, societal and political perspective - has expanded significantly since its adoption 20 years ago.

In particular, the evolution of the digital services landscape has been characterized (in the EU as well as globally) by the emergence of big online platforms which benefit from strong network effects and whose business model is based on the continuous extraction and analysis of users' data for profiling purposes. These platforms - which exert an unprecedented economic and societal impact - have become as a matter of fact public spaces, where individuals share and access information, where businesses reach their customers and where politicians and public authorities communicate with citizens.

At the same time, the transformation of digital services into increasingly complex environments has been accompanied by the dissemination of illegal content (such as illegal hate speech and terrorist content) and illegal goods (such as counterfeit or unsafe products). Furthermore, digital services have enabled the publication and dissemination of harmful (although not necessarily illegal) content, such as online disinformation, with major political and societal consequences.

In response to the challenges connected to the proliferation of illegal content, goods, and services, the EU has adopted over the past years a variety of initiatives, including sector-specific legislation (see Section 1.3.1), non-binding guidelines for platforms to tackle illegal content online[6] and measures based on self-regulatory cooperation[7]. These initiatives have to a certain extent complemented the e-Commerce Directive and have increased awareness on the risk and harms brought by the digital transformations, including as regards the implications for the protection of fundamental rights. However, as acknowledged by the Commission, such interventions inevitably fail to address the systemic societal risks posed by digital services and online platforms in particular. Crucially, the lack of updated and harmonized rules hinders appropriate levels of protection for fundamental rights, adding legal uncertainty and fragmentation to an already complex regulatory landscape.

---

[5] The term "information society services" is defined by Article 2(a) DSA proposal as having the meaning of Article 1(1)(b) of the Transparency Directive 2015/1535, "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

[6] European Commission, Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final)

[7] Such as for instance the 2018 Code of conduct on countering illegal hate speech online, the 2019 Joint Action of the consumer protection cooperation network authorities and the EU Internet Forum against terrorist propaganda online launched in 2015. See DSA Inception Impact Assessment, 2020, p. 1., available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-internal-market-and-clarifying-responsibilities-for-digital-services_en

1.2.2. A fragmented landscape: regulatory initiatives of the Member States

In the past years, Member States have increasingly introduced legislation on digital services and online platforms in an effort to supervise them and reduce the harms associated with the spread of illegal content and goods. One of the main drivers of the DSA proposal is therefore the urgency to limit the normative fragmentation resulting from the initiatives undertaken at the national level. For instance, as pointed out in the DSA Impact Assessment, some Member States have introduced notice-and-action procedures in their legislation, particularly in the area of copyright infringements; some others have defined counter-notice procedures and forms of alternative dispute settlement.[8] More recently, national laws such as the German NetzDG[9], the French Avia Law[10] and the Austrian KoPlG[11] have imposed more stringent obligations on the platforms, requiring them, under the threat of high fines, to ramp up their efforts in limiting the spread of certain types of illegal content, including illegal hate-speech. All these national level initiatives have caused fragmentation and legal uncertainty on the liability regime applicable to providers, affecting in particular smaller service providers and hindering their capability to compete effectively on the market.

1.2.3. Pre-proposal consultations with stakeholders

The DSA proposal follows numerous consultations undertaken by the Commission over the years with a wide variety of stakeholders (including digital service providers, other businesses, academia, public authorities, civil society organization and citizens). While stakeholders have generally agreed on the need to update the current set of rules, they have also broadly supported the idea that the key principles of the e-Commerce Directive (in particular, the liability exemptions and the prohibition of general monitoring), are still valid today and should be transferred in the new DSA regulation. As explained in the memorandum accompanying the DSA proposal, in light of the implications for freedom of expression, stakeholders also agreed that the DSA should not define harmful (but not necessarily illegal) content and that removal obligations should only apply to illegal content.[12]

In October 2020, the European Parliament adopted three resolutions on the planned DSA proposals.[13] These resolutions called for transparency and accountability for digital services providers and demanded effective obligations to tackle illegal content online. They also called for increased oversight at EU and national level as well as cross-border cooperation between the competent authorities in enforcing the law.

---

[8] See Impact Assessment accompanying the Proposal for a Digital Services Act, SWD (2020) 348 final, p. 28-29, available at: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-services-act.

[9] German Network Enforcement Act (Netzwerkdurchsetzungsgesetz or "NetzDG") of 30 June 2017.

[10] French"Avia" Law 2020-766 of 24 June 2020 on online hateful content.

[11] Kommunikationsplattformen-Gesetz (KoPl-G) Bill, presented by the Austrian government on 3 September 2020.

[12] Explanatory Memorandum to the DSA proposal (see footnote 1), page 9.

[13] European Parliament, Resolution on improving the functioning of the Single Market (2020/2018(INL)); European Parliament, Resolution on adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)); European Parliament, Resolution on the Digital Services Act and fundamental rights issues posed (2020/2022(INI)).

In particular, the resolutions of the European Parliament took a strong stance on the core business model underpinning online platforms. Highlighting the negative impact of personalised advertising - particularly micro-targeted and behavioural advertising[14], notably relying on pervasive user's tracking and big data - the resolutions recommended the adoption of stricter rules on targeted advertising, in favour of less intrusive (contextual) forms of advertising[15]. Specifically, the EP recommended to subject behavioural advertising to the users' freely given, specific, informed and unambiguous consent and invited the Commission to consider "a phasing out, leading to a prohibition" of targeted advertisement[16].

1.2.4. The Digital Services Act: objectives, policy options and scope

With the DSA proposal, the European Commission aims to ensure an optimal provision of cross-border digital services in the internal market, by overcoming existing legal fragmentation and regulatory gaps. According to the Commission, clearer rules are crucial to tackling online harms and ensuring a safer online experience, where users' fundamental rights enjoy adequate level of protection. Achieving these objectives requires setting up a solid regulatory architecture, where national competent authorities are capable in practice of policing the behavior and policies of service providers, particularly online platforms, and cooperate effectively among each other.

The proposed regulation is accompanied by an Impact Assessment report,[17] which illustrates the policy options and describes the wider policy context. As explained in the Impact Assessment, the Commission considered three main policy options. The first one would introduce procedural requirements for intermediaries with regard to illegal activities and reinforcing the cooperation mechanisms to address cross-border supervision issues. The second option, in addition to the measures foreseen in this first option, would introduce fully harmonized measures to promote respect of fundamental rights and transparency on advertising and harmonize conditions for the removal of illegal content. The third option, adding to the remedies of the previous ones, consisted in adopting an asymmetric approach with enhanced obligations for very large platforms, clarifications for the exemption from liability for intermediaries and a governance system characterized by stronger regulatory supervision and enforcement. The EC's assessment identified the third option as the most effective and proportionate in addressing the challenges posed by evolving digital services and very large online platforms in particular.

As set forth by art. 1 of the DSA proposal, the draft regulation introduces a horizontal framework applicable to all intermediary services. Specifically, the DSA establishes rules on:

a) the conditional exemption from liability of providers of intermediary services;

[14] Resolution on improving Single Market, para 33; Resolution on the DSA and fundamental rights, para 9; Resolution on adapting commercial and civil law rules, para 14.
[15] Resolution on adapting commercial and civil rules, para 15; Resolution on improving Single Market, para 33.
[16] Resolution on adapting commercial rules para 15 and 17; Resolution on improving single market, p. 26.
[17] Impact Assessment accompanying the Proposal for a Digital Services Act, SWD (2020) 348 final.

b) targeted asymmetrical due diligence obligations for a more transparent and safer online environment. Some of these obligations apply to all intermediaries, some other additional obligations are applicable to providers of hosting services and to online platforms. A last category of measures applies - in addition to the already mentioned obligations - only to very large online platforms and addresses the management of the systemic risks these platforms pose from a societal and economic perspective;
c) the implementation and enforcement of the Regulation, including as regards the cooperation between the competent authorities (the Digital Services Coordinators, reunited in a body called European Board for Digital Services).[18]

1.3. The relation between the DSA and other legal instruments applicable to digital services

1.3.1. Pre-existing EU sector-specific initiatives on illegal and harmful content online.

In an attempt to address the challenges posed by a fast-evolving digital services ecosystem, a number of sector-specific legislative initiative have been proposed or adopted at the EU level over the last years. These initiatives appear limited in scope, as they tackle specific types of illegal content (for instance, terrorist content, child abuse material, illegal hate speech, copyright infringement or counterfeited or dangerous products) and/or they do so on a specific sub-set of services (for instance audiovisual services and platforms).[19] As a result, these interventions fail to provide horizontal rules (in terms of obligations, responsibilities and regulatory oversight) on the effective and fundamental rights-compliant management of illegal content, which makes the need for new legislation particularly urgent. However, as explained in the explanatory memorandum, the DSA is not intended to replace, but rather to complement, these sectoral initiatives, which will continue to apply as *lex specialis*.
Sector-specific legislation that will remain in force alongside the DSA includes the 2018 revised Audiovisual Media Services Directive[20], which introduced new rules on video-sharing platforms with regard to audiovisual content and audiovisual commercial communications, as well as the Platform to Business Regulation[21], which imposed transparency obligations on platforms *vis à vis* their business users and required to provide those users with effective complaint mechanisms.

[18] Article 47 DSA establishes an independent advisory group of Digital Services Coordinators (DSCs) named 'European Board for Digital Services' (the 'Board').
[19] Impact Assessment, para. 103.
[20] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.
[21] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

Another significant development in the EU policy concerning online content regulation took place a couple of days before the presentation of the DSA proposal, when the Council Presidency and the European Parliament reached a provisional agreement on a draft regulation on addressing the dissemination of terrorist content online (TERREG).[22] The text sets out the obligation for intermediary to remove within one hour any content which has been signaled as "terrorist content". The final approval of the TERREG proposal took place in April 2021.[23]
Sectoral instruments are not limited to those tackling content, products or services of illegal nature. Over time, the EU has also been adopting a series of tools, including voluntary cooperation, to increase the pressure on online platform to increase their efforts in moderating harmful (but not necessarily illegal) content. Following the report of a high-level expert group on fake news and online disinformation, [24] in 2018 the Commission issued a Communication on the EU approach to tackling online disinformation.[25] The Communication led to the adoption of a Code of Practice on Disinformation, [26] joined by the main online platforms and trade associations from the advertising industry. In September 2020 the Commission published an assessment[27] of the Code of Practice, which highlighted a series of shortcomings in the current Code, consisting in particular in the lack of precise commitments, meaningful key performance indicators (KPIs) and access to data allowing for an independent monitoring of the signatories' compliance and research on disinformation.

1.3.2. The EU Democracy Action Plan

The DSA proposal is intended to be complemented by further legislative developments and measures adopted under the European Democracy Action Plan,[28] a policy framework presented by the European Commission in early December 2020, days before unveiling the DSA package. The European Democracy Action Plan aims to address the challenges posed to democracy, in the EU and on a global scale, by the digital transformations.[29] The action plan, which is connected to the protection of fundamental rights, and the principles of transparency and accountability (in relation to online services), defines an EU framework, articulated around

[22] https://www.consilium.europa.eu/en/press/press-releases/2020/12/10/terrorist-content-online-council-presidency-and-european-parliament-reach-provisional-agreement/
[23] European Parliament legislative resolution of 28 April 2021 on the Council position at first reading with a view to the adoption of a regulation of the European Parliament and of the Council on addressing the dissemination of terrorist content online, available at: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0144_EN.html
[24] Report of the independent High Level Expert Group on fake news and online disinformation, *A multi-dimensional approach to disinformation*, 12 March 2018.
[25] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee, and the Committee of the Regions on *Tackling Online Disinformation: a European Approach*, of 26 April 2018, COM(2018) 236 final.
[26] EU Code of Practice on Disinformation, 2018, available at: https://ec.europa.eu/digital-single-market/en/code-practice-disinformation.
[27] European Commission, Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement, SWD (2020) 180 final, available at: https://ec.europa.eu/digital-single-market/en/news/assessment-code-practice-disinformation-achievements-and-areas-further-improvement
[28] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee, and the Committee of the Regions on the European Democracy Action Plan ("European Democracy Action Plan"), 3 December2020, COM(2020) 790 final.
[29] Ibid, p. 2.

specific measures, to achieve three main objectives. These are the protection of the integrity of elections and democratic participation, the promotion of free and independent media and the tackling of disinformation.[30] In particular, the Commission foresees an active role for the DSA in contributing to the actions under the first and the third of these goals.

As regards the objective of protecting the integrity of elections and fostering democratic participation, the envisaged measures include two proposals by the Commission in 2021. One concerns the transparency of political advertising and is supposed to supplement the rules on online advertising set forth by the DSA, while the other one addresses illegal content online through the extension of the list of EU crimes under art. 83(I) TFEU to comprise hate crime and hate speech (including online).

The combination of the European Democracy Action Plan and the DSA proposal is considered a pivotal point in the policy pursued over the last years against disinformation.[31] Among the identified actions to counter disinformation, the Action Plan mentions the co-regulatory backstop of the DSA for the measures to be included in a strengthened version of the 2018 Code of practice on disinformation, which will be revised on the basis of the guidance issued by the Commission in May 2021.[32] Such goals include: measuring the impact of disinformation and the effectiveness of the platforms' policies (including through KPIs), reducing the monetization of disinformation connected to advertisement on online platforms, introducing transparent standards for fact-checking and ensuring access to disinformation-related data to researchers.[33]

1.3.3. The Digital Markets Act ("DMA")

As part of a wider package of rules for digital services, on the same day that the DSA proposal was made public, the Commission also unveiled a Proposal for a Regulation on contestable and fair markets in the digital sector, the Digital Markets Act ("DMA")[34]. The DMA contains the new competition law instruments (*ex ante* rules) announced earlier by the Commission.[35] The DMA complements the provisions of the DSA, addressing in particular the role and the unfair practices operated by certain core online platforms which meet the definition of "gatekeepers". These are platform services consisting in activities such as online intermediation, search engines, social networks, video-sharing, number-independent interpersonal communication services, operating systems, cloud computing, advertising, etc.

---

[30] Ibid, p. 4.

[31] Paolo Cesarini, *Regulating Big Tech to Counter Online Disinformation: Avoiding Pitfalls while Moving Forward*, Media Laws (2021), p. 2, http://www.medialaws.eu/wp-content/uploads/2021/02/Cesarini.pdf

[32] European Commission, *Guidance on Strengthening the Code of Practice on Disinformation*, (COM (2021) 262 final), available at: https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation.

[33] European Democracy Action Plan, p. 23.

[34] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final.

[35] See Crémer, J., de Montjoye, Y.A. and Schweitzer, H., *Competition policy for the digital era. Report for the European Commission*, 2019, available at: https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf

The DMA introduces a set of quantitative parameters to presume that a large online platform qualifies as "gatekeeper" based on the following criteria:

i. significant impact on the internal market and activity in multiple EU countries;
ii. provision of a core platform service, which connects a large end user base to a large number of businesses;
iii. it has (or is about to have) an entrenched and durable position in the market.[36]

Pursuant to art. 5 and 6 of the proposed DMA, the gatekeepers will have to comply with a series of obligations concerning the practices that limit contestability or are unfair. Specifically, gatekeepers will be obliged to refrain from a series of conducts, which include: combining the personal data from their core services with the personal data sourced from other services offered by them or by third parties; requiring the business users to use identification services of the gatekeeper for services they offer through the gatekeeper's core platform services; making the use of a core platform service by business users and end users conditional upon the subscription to another core platform services; using data generated on the platform by business users in competition with the latter and discriminating in rankings products and services offered by third parties.
The DMA proposal also foresees situations where the Commission, in exceptional circumstances, can suspend the obligations under art. 5 and 6 for an individual core platform service[37] or where an exemption can be granted for overriding reasons of public interest[38]. The draft Regulation also sets forth the obligation to notify any intended concentration[39] and the obligation to submit to an independent audit any technique for profiling of consumers applied by the gatekeeper across its core platform services[40].
In case of non-compliance, the Commission can adopt non-compliance decisions and impose fines as well as periodic penalty payments.

1.4. The Digital Compass, EU ambitions for 2030

Following the Special European Council meeting of October 2020 - dedicated to the pillars of EU's recovery from the Covid-19 pandemic - EU leaders called on the Commission to present, by March 2021, a "Digital Compass" plan setting out the EU's digital goals for 2030.
As it was established that at least 20% of the funds made available under the Recovery Facility must be devoted to the digital transition, the Commission is expected to present a strategy to achieve a number of ambitious objectives. Such goals fall under a series of key policy areas, which include digital services and online platforms. Other priority areas are: next generation digital technologies (including quantum computing and cloud), sovereignty in strategic digital value chains (especially microprocessors), artificial intelligence, cybersecurity, connectivity, eHealth, digitalization of justice and climate neutrality.

[36] Article 3 DMA proposal.
[37] Article 8 DMA proposal.
[38] Articlre 9 DMA proposal.
[39] Article 12 DMA proposal.
[40] Article 13, DMA proposal.

While the Commission addressed the digital services and online platform strategic area with the DSA proposal, the main development in the area of the data economy is represented by the proposal for a Regulation on European Data Governance (the "Data Governance Act")[41].
The proposal, presented by the Commission on 25 November 2020, is the first of a series of measures announced in the context of the 2020 Digital strategy for data. The proposal aims to encourage the availability of data for reuse across sectors (particularly in strategic areas such as such energy, mobility and health), by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. Specifically, the stated goals of the proposed Data Governance Act regulation include: making public sector data available for re-use, in situations where such data is subject to rights of others; promoting the sharing of data among businesses; allowing the use of personal data through the assistance of 'personal data-sharing intermediaries'; and allowing use of data made available for 'altruistic' purposes.

[41] Proposal for a Regulation of the European Parliament and of the Council on European Data Governance ("Data Governance Act"), COM (2020), 767 final.

2. The Digital Service Act proposal – An overview

2.1. Introduction

This part of the discussion paper provides a critical overview of the overall architecture and specific rules of the DSA draft regulation presented by the Commission in December 2020.

The description of the relevant provisions follows the structure of the DSA proposal and is complemented by a discussion of the relevant legal and policy context. Giving account of the positions expressed by a variety of stakeholders in reaction to the DSA proposal, this overview sets out to identify and highlight aspects of the proposal where clarifications, refinement or re-consideration might be needed, including relevant suggestions for amendments of the current provisions.

2.2. Scope and definitions

A key innovation in relation to the e-Commerce directive is to be found in the extra-territorial scope of the draft DSA regulation. The DSA will apply to intermediaries offering their services to users who are established or resident in the EU, regardless of where the service provider is established.[42] As under GDPR, intermediaries not based in the EU will have to appoint a legal representative in the EU.[43]

Among the definitions included under Article 2, the definitions of illegal content and online platform, not included in the e-Commerce directive, are of particular relevance. The DSA's definition of "illegal content" consists of a broad reference to other relevant provisions of law, as it is intended as meaning "any information, which, in itself or by reference to an activity, […], is not in compliance with Union law or the law a Member State, irrespective of the precise subject matter or nature of that law".[44]

An "online platform" is defined as a hosting service provider which, upon users' request, "stores and disseminates to the public information, unless that activity is a minor or purely ancillary feature of another service", which cannot operate technically without the latter service.[45]
The current definition of online platforms, as including the requirement of 'dissemination to the public', raises a number of questions, particularly as regards the position of certain hosting services such as infrastructural cloud service providers. In particular, it is not clear if this requirement intends to exclude service providers that do not have consumers as their direct

[42] Article 1(3) DSA proposal
[43] Article 11 DSA proposal.
[44] Article 2(g) DSA proposal.
[45] Article 2(h) DSA proposal.

contractual counterparts.[46] Another element of the definition which needs clarification concerns who should be considered the recipient of the service: whether the application provider in direct contractual relationship with the cloud service, or the contributor to the application, or the general public accessing the application hosted on the cloud.[47] These interpretative doubts are particularly relevant, also in consideration of the fact that the definition - and related due diligence obligations - of "very large online platforms" (VLOPs) builds upon the definition of "online platforms". Finally, there is the question of whether the particular online platform could in effect contain multiple online services (for instance the consumer facing social media platform service in combination with an advertiser-facing advertisement service) and what this would mean for the application of the relevant definitions to the service as a whole.

In October 2021, the European Parliament's Committee on Legal Affairs (JURI) adopted its final opinion on the DSA proposal.[48] The JURI opinion proposes, under Article 1, to include in the scope of the draft Regulation "the instant messaging services used for purposes other than private or non-commercial". The proposal has been harshly criticized by digital rights activists, as it would be impossible for service providers to ascertain the type of use of the messaging service - and then potentially exempt the content at issue from DSA obligations - without violating the privacy and encryption of communications.[49]

2.3. Liability of intermediaries

2.3.1. General monitoring and safe harbors (Articles 3, 4, 5 and 7)

The DSA proposal maintains the key principles set out by the e-Commerce directive concerning the liability regime of providers of intermediary services and the prohibition of general monitoring.

Specifically, the prohibition of imposing general monitoring and active fact seeking obligations on the intermediaries, set forth by article 15(1) e-Commerce directive, is transposed in the draft Regulation by Article 7 of the DSA proposal. On the other hand, Articles 3, 4 and 5 of the

[46] European Parliament, Committee on the Internal Market and Consumer Protection (IMCO), Background Paper for the workshop *"The Digital Services Act and the Digital Markets Act: A forward-looking and consumer-centred perspective"*, p. 5, available at: https://www.europarl.europa.eu/cmsdata/234761/21-05-19%20Background%20note%20REV%20final.pdf.

[47] Ibid.

[48] European Parliament, Committee on Legal Affairs (JURI), *Opinion on the proposal for a regulation of the European Parliament and of the Council on Single Market for Digital Services (Digital Services Act)*, Rapporteur Jeoffroy Didier, 11 October 2021, available at: https://www.europarl.europa.eu/doceo/document/JURI-AD-694960_EN.pdf

[49] See EDRI, *DSA should tackle the root cause of polarization, not just its symptoms*, available at: https://edri.org/our-work/dsa-should-tackle-the-root-cause-of-polarisation-not-just-its-symptoms/; Patrick Breyer, *Digital Services Act: Legal Affairs Committee attacks user privacy and free speech online*, 30 September 2021, available at: https://www.patrick-breyer.de/en/digital-services-act-legal-affairs-committee-attacks-user-privacy-and-free-speech-online/

proposal - which respectively define the conditions for the exemption from liability for the providers offering "mere conduit", "caching" or "hosting" services - reproduce Articles 12, 13 and 14 ("safe harbours") of the e-Commerce directive.

As a relatively minor adjustment, article 5(3) DSA introduces new conditions as regards the liability exemption of online platforms intermediating between consumers and traders (online marketplaces). In particular, an online marketplace would be liable under consumer law where it would cause an average consumer to consider that the object of the transaction is provided directly by the platform or by a user under its authority or control. The introduction of this exception, applicable to marketplaces, to the liability regime governing other intermediary services was welcomed by the European Consumer Organization (BEUC). At the same time, BEUC highlighted that this provision does not create any positive secondary liability for the marketplaces[50]. Therefore it called on the co-legislators to amend article 5.3 to establish the joint and severable liability of online marketplaces and traders in a series of circumstances, including non-compliance of their due diligence obligations, damages, non-performance of the contract and guarantees. [51]

The European Parliament Committee on the Internal Market and Consumer Protection (IMCO), lead committee for the DSA, published a draft report on the DSA proposal at the end of May 2021.[52] The final IMCO report should be adopted in November 2021. Some of the most notable amendments to the original proposal, included in the IMCO report, concern the safe harbour provisions, with the imposition of deadlines on the hosting services to carry out removals of illegal content. Specifically, upon acquiring actual knowledge or awareness of certain illegal content, providers of hosting services would have to remove it as soon as possible, and in any case within 24 hours, if the illegal content at issue "can seriously harm public policy, public security or public health or seriously harm consumers' health or safety".[53] In all other cases, when the content in question does not pose a risk of such harms, the removal must take place within seven days.[54]
The JURE opinion as well introduces fundamental changes to the liability regime established under the e-Commerce directive and the original DSA proposal, imposing extremely short removal deadlines. Specifically, Article 5 of the JURI proposal requires intermediaries to remove illegal content "as soon as possible and in any event": i) within 30 minutes if it is the broadcast of a live sport or entertainement event; ii) within 24 hours if it has the potential to "harm public policy, public security or public health or seriously harm consumers' health or

[50] The European Consumer Organisation (BEUC), The Digital Services Act – BEUC position paper, p. 9-12, available at: https://www.beuc.eu/publications/beuc-x-2021-032_the_digital_services_act_proposal.pdf
[51] Ibid. See also comments under article 22 DSA on traceability of traders, p. 24-25.
[52] European Parliament, Committee on the Internal Market and Consumer Protection (IMCO), Draft Report on the proposal for a regulation of the European Parliament and of the Council on a Single Market for European Digital Services (Digital Services Act) and amending directive 2000/31/, available at https://www.europarl.europa.eu/doceo/document/IMCO-PR-693594_EN.pdf
[53] IMCO Committee draft report on the DSA, Art. 5, new par. 1(a).
[54] Ibid.

safety"; iii) within 72 hours in all other cases where the content does not seriously harm the elements listed under ii).[55]

From these recent developments in the Parliament, it is clear that the question of timeframes in the liability regime of hosting services will become one of the most debated and contentious elements of the DSA negotiations, particularly for the impact that these can have on freedom of expression and other fundamental rights by creating a strong incentive for the providers to over-remove content, including through the intensification of automated content moderation.

2.3.2. Own-initiative investigations (Article 6)

A notable addition of the DSA to the intermediary liability regime set out by the e-Commerce directive (and transferred in the draft regulation under Articles 3,4 and 5) is Article 6 on own-initiative investigations. Pursuant to Article 6, intermediaries will not automatically lose (will not be "deemed ineligible from") the conditional exemption from liability "solely because" they engage in voluntary investigations or other initiatives for "detecting, identifying and removing, or disabling access to, illegal content" or to ensure compliance with other provisions of EU law, including those stemming from the DSA.

The scope of Article 6 DSA is clarified by recital 25, which provides that "the mere fact that providers undertake such activities does not lead to the unavailability of the exemptions from liability," if those activities are undertaken "in good faith and in a diligent manner". The same regime applies to the measures undertaken in good faith by intermediaries to enforce their terms and conditions, involving content that is contrary to their contractual terms and community guidelines but not necessarily illegal.[56]

The background of the legislative evolution represented by Article 6 is to be found in the fact that while Article 7 DSA (corresponding to Article 15 e-Commerce Directive) prohibits the imposition on intermediaries of an obligation of general monitoring, still over the past years intermediaries have been increasingly pressured by policymakers to step-up their efforts in policing content through voluntary initiatives.[57] The many uncertainties surrounding the scope and implications of own initiatives, however, have created concerns about the legal consequences of voluntary investigations for intermediaries, as such initiatives have the potential to trigger knowledge and therefore compromise the intermediaries' capability to invoke the liability exemptions.[58]

[55] JURI Committee opinion on the DSA, Article 5, new paragraph 1(a).
[56] Recital 25 DSA proposal.
[57] Kuczerawy A., *The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act*, Verfassungsblog, 2021, available at: https://verfassungsblog.de/good-samaritan-dsa/
[58] Van Hoboken, J. and others, Hosting intermediary services and illegal content online: An analysis of the scope of Article 14 ECD in light of developments in the online service landscape. Final report prepared for the European Commission, 2018, available at https://op.europa.eu/nl/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1

The ratio of Article 6 DSA is therefore to incentivize intermediaries to engage in the voluntary policing of content which is illegal or contrary to their terms and conditions by stating that such actions - where taken in good faith and diligently- do not automatically rule out the safe harbour protection. The current phrasing of Article 6, however, leaves several interpretative questions open, which have the potential to undermine the incentive system designed by the Commission and the legal certainty on which such system is founded. Uncertainties exist, for instance, with respect to the meaning of "solely",[59] the consequences of the knowledge gained through an own investigation and how the assessment of diligence could be impacted by the unsuccessful outcome of a voluntary investigation.[60] Another policy objective which could be frustrated by Article 6 is that of carrying out content moderation in due observance of the fundamental right to freedom of expression. In this regard, reactions to the proposal converge on the conclusion that this provision may translate into more undue content removals.

It has been debated whether Article 6 DSA introduces in the EU liability framework a type of protection for intermediaries which corresponds to the one granted under the Communications Decency Act (CDA) Section 230 under U.S. law, known as "Good Samaritan" protection. According to Section 230, intermediaries should not be held liable for voluntary actions taken in good faith for content which can be considered objectionable on several grounds. The scope of Section 230 is much wider than that of Article 6 DSA, as it offers absolute immunity to intermediaries non only when they undertake voluntary initiatives, but also when - because of a decision or just by mistake - they do not take action against such content.[61]

2.3.3. Orders to act against illegal content (Article 8) and orders to provide information (Article 9)

The DSA proposal defines the obligations of the intermediaries with regard to two categories of orders issued by national judicial or administrative authorities: orders to act against illegal content and orders to provide information. When intermediaries receive an order under Articles 8 and 9, issued by the relevant national authority, to act against a specific piece of illegal content or to provide information about a specific user, they must promptly inform such authority of the actions taken to comply with the order.

The orders to act against illegal content and to provide information must include, respectively:

a) a reference to the specific legal provision infringed and an indication about the territorial scope of the order;[62]

[59] Barata J., *The DSA and the reproduction of old confusions*, Verfassungsblog, 2021, available at: https://verfassungsblog.de/dsa-confusions/
[60] Kuczerawy, *The Good Samaritan that wasn't,* Verfassungsblog, 2021.
[61] Ibid.
[62] Article 8.2, letters a) and b) DSA proposal.

b) an explanation of the objective of the information requested and why it is "necessary and proportionate" to decide whether users complied with EU or national rules, "unless such a statement cannot be provided for reasons related to the prevention, investigation, detection and prosecution of criminal offences".[63]

Both orders must also provide information about redress available to the service providers and to the users. Furthermore, these orders envisage the involvement of the Digital Services Coordinators (DSCs), the regulatory authorities to whom enforcement functions are assigned under the DSA. A copy of the orders issued under Articles 8 and 9 must be transmitted by the Digital Services Coordinator (DSC) of the Member State where the authority issued the order to all other Digital Services Coordinators through the system established under Article 67.

Articles 8 and 9, together with other DSA provisions commented further in this part of the paper - such as Article 19 on trusted flaggers; and article 21 on notification of suspicions of criminal offences - reflect the tendency to involve private actors (i.e., the platforms) in enforcement initiatives.

2.4. Due diligence obligations and transparency (Chapter III DSA)

2.4.1. A tiered system of obligations

Chapter III of the DSA sets out a system of tiered and due diligence obligations which are meant to adapt to the different types and nature of the intermediary services concerned.[64] Some of these obligations apply to all intermediaries (Section I, Articles 10-13). Additional obligations are applicable to providers of hosting services, including online platforms (Section II, Articles 14 and 15) and further additional rules tackle online platforms (Section III, Articles 16-24). A last category of asymmetrical measures applies - in addition to the already mentioned obligations - only to very large online platforms, "VLOPs" (Section IV, Articles 25-33) and addresses the management of the systemic risks their services can create.

The scope of application of these tiered obligations is one of the most significant design aspects of the DSA draft regulation and a debate is unfolding around the definitions and categorizations set out by the proposal.

According to DIGITALEUROPE, the organization that represents all the major technology companies (including the so-called "GAFAM"), the current DSA definition of online platforms is too broad. The industry organization advocates for a restriction of this definition, to expressly exclude providers such as IT infrastructure services, which typically have no direct visibility over how customers manage their content, and cloud-based hosting services, which store

[63] Article 9.2 DSA proposal.
[64] Recital 35 DSA proposal.

customers' content but do not have dissemination of such content as their main feature.[65] As explained in Section 2.2, their status under the DSA provisions on online platforms and VLOPs is not clear.

BEUC, on the other hand, criticized the exclusion of "small" enterprises (article 16 DSA) from the set of obligations applicable to online platforms, arguing that such exclusion would deprive the DSA of much of its desired impact.[66] Considering that an enterprise with up to 50 employees and up to 10 million turnover qualifies as small enterprise, it can be argued that at least some of the key obligations of Section II of Chapter III DSA (internal complaint and out-of-court dispute settlement; traceability of traders; online advertising and recommender systems) should not be covered by this exclusion and should therefore apply to small enterprises.
Because of its political characterization, the question of the position of the SMEs within the DSA framework is emerging as one of the most contentious issues in the parliamentary debates. For instance, the recent JURI Committee's opinion introduces a new Article 10 which allows intermediaries, under certain circumstances, to apply to the Commission for a waiver on the requirements of Chapter III DSA. Such waiver can be granted when these intermediaries are either micro, small and medium enterprises, or medium enterprises without systemic risks connected to illegal content, or editorial platforms as defined under the new Article 2(hb) of the opinion.[67]

As discussed further under Section 2.5, the parameters set out by the Commission proposal to identify VLOPs have been met with some criticism, which also translated in significant proposals for amendments in the relevant parliamentary Committees.

2.4.2. Provisions applicable to all intermediaries

2.4.2.1. Single point of contact (article 10) and legal representative (article 11)

The DSA proposal requires intermediaries to identify a single point of contact for communication with Member States authorities, Commission and the Board. Moreover, if not established in the EU, providers must appoint a legal representative in one of the Member States where they offer services. The representative can be held liable for non-compliance with the Regulation, with no prejudice to the liability of the intermediaries.

2.4.2.2. Terms and conditions (Article 12)

[65] DIGITALEUROPE, Digital Services Act position paper, p. 6-7, available at: https://www.digitaleurope.org/wp/wp-content/uploads/2021/03/FINAL-DSA-Paper-March-2021-1.pdf
[66] BEUC position paper on the DSA, p. 15.
[67] JURI Committee opinion on the DSA, Article 10.

Intermediaries must provide information, in their terms and conditions, on the content moderation activities undertaken on their services. They must explain in clear and unambiguous language how content moderation is carried out, i.e. which measures and tools, including algorithmic decision-making and human review, are applied to this purpose. Article 12(2) of the proposal requires intermediaries to apply the abovementioned restrictions *"in a diligent, objective and proportionate way"* and "*with due regard to the rights and legitimate interests of all parties involved, including the applicable fundamental rights of the recipients of the service as enshrined in the Charter"*.

The EDPS recommended including specific language on the fact that content moderation should be undertaken whenever possible without processing personal data, and that the proposal should also detail the precise circumstances which justify such processing for the purposes of countering illegal content.[68] It also suggested to extend the requirements of Article 12(2) (fundamental rights safeguards) to all content moderation activities, not just the ones undertaken on the basis of terms and conditions, and to require that any restriction applied to content must be both proportionate and *necessary*, in accordance with the principles of data minimization and data protection by design and by default.[69]
As discussed by Appelman et al, it is unclear whether the current wording of Article 12 DSA requires intermediaries to apply EU fundamental rights law, including the right to freedom of expression, in content moderation decisions that are based on terms and conditions. [70] They signal the risk that, where the legislative text remains unchanged, the obligations envisaged under Article 12 remain a "paper tiger", as the scope of application and enforcement of Article 12 will only become clear and effective if and when courts are called to interpret it.[71] Considering the exceptional power of VLOPs' in content moderation, it is reasonable to argue that Article 12 could clarify that fundamental rights are applicable in the horizontal relation between them and the users, and require VLOPs to apply human rights law standards in the moderation of online content.[72]

2.4.2.3. Transparency (article 13)

[68] European Data Protection Supervisor (EDPS), Opinion 1/2021 on the Proposal for a Digital Services Act, p. 9, available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act_en
[69] Ibid., p. 13.
[70] For a systematic analysis of art. 12 DSA and its context, see Appelman N., Quintais J. P. and Fahy R., *Article 12 DSA: Will platforms be required to apply EU fundamental rights in content moderation decisions?*, available at: https://dsa-observatory.eu/2021/05/31/article-12-dsa-will-platforms-be-required-to-apply-eu-fundamental-rights-in-content-moderation-decisions/
[71] Appelman, N., Quintais, J. P.; Fahy, R.: *Using Terms and Conditions to apply Fundamental Rights to Content Moderation: Is Article 12 DSA a Paper Tiger?*, in Richter, H., Straub, M. and Tuchtfeld, E., *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package* (October 11, 2021), Max Planck Institute for Innovation & Competition Research Paper No. 21-25, Available at SSRN: https://ssrn.com/abstract=3932809
[72] Buri, I., Van Hoboken, J., *The DSA Proposal's Impact on Digital Dominance* , in Richter, H., Straub, M. and Tuchtfeld, E., *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package* (October 11, 2021), Max Planck Institute for Innovation & Competition Research Paper No. 21-25, Available at SSRN: https://ssrn.com/abstract=3932809

Intermediaries, with the exception of micro and small enterprises, are required to publish, *"at least once a year, clear, easily comprehensible and detailed reports"* on their content moderation activity performed in the period of reference. The reports must provide specific information on a series of elements listed under Article 13: the number of orders received from Member States' authorities (distinguishing the type of illegal content at issue); the number of notices submitted pursuant to the notice and action procedure; the type of content moderation measures undertaken on their own initiative and the complaints received through the internal complaint-handling system.

The reporting obligations detailed under Article 13 are complemented by the additional obligations provided for under Article 23 and 33, which apply, respectively, to online platforms and to VLOPs.

Warning about the risk that these transparency reports might be structured strategically, BEUC recommended including additional rules on the structure, content, (objective) terms and methodology to be followed by intermediaries when complying with these obligations.[73]

2.4.3. Additional provisions applicable to providers of hosting services, including online platforms

2.4.3.1. Notice and action (Article 14) and statement of reasons (Article 15)

Article 14 DSA proposal requires providers of hosting services, including online platforms, to set up a "notice-and-action" mechanism through which any individual or entity can notify them of the presence on their services of specific pieces of content that they consider illegal.

Notices of (alleged) illegality are considered sufficiently precise and substantiated when they include all of the elements listed under Article 14(2) DSA:

i. the reasons why the content is considered to be illegal;
ii. its electronic location;
iii. name and email of the notifier;
iv. a good faith belief statement.

Notices that include the above-mentioned elements - relating to an alleged, yet unassessed, illegality of the content at issue - are considered to give rise to actual knowledge or awareness for the purposes of intermediary liability. It is safe to assume that the threat of liability will induce many platforms to adopt a "delete first, think later" type of approach,[74] leading to the over-removal of legal content and to a later re-assessment of the removal (only if and where a user challenges the takedown).

[73] BEUC position paper on the DSA, p. 20.
[74] EDRI, *Delete first, think later*, 2021, available at: https://edri.org/our-work/delete-first-think-later-dsa/

The service provider must confirm receipt of the notice and indicate whether automated means will be used for processing the notice or taking the decision. The notifier must be informed, without undue delay, of the decision taken and on how to challenge that decision.

If a service provider decides to remove or disable access to specific pieces of content, it must inform the user and provide a statement of the reasons supporting that decision. Such statement must include at least the elements listed under Article 15(2):

i. the outcome and scope of the decision;
ii. the facts and circumstances taken into consideration for the decision;
iii. information on the use of automated decision-making means;
iv. for allegedly illegal content, a reference to the legal ground relied on and explanations as to why the information is considered to be illegal;
v. where the decision is based on the alleged incompatibility of the information with the terms and conditions, a reference to the contractual ground relied on and explanations;
vi. information on the possibilities available to the user to challenge the decision (internal, out-of-court and judicial redress mechanisms).

As regards the use of automated means for content moderation or decision-making purposes (Articles 14(6) and 15(2)(c) DSA), the EDPS recommended imposing additional transparency obligations on hosting services to provide further details on the technology employed and the criteria informing their decision.[75] More in general, the EDPS repeatedly warned about the risk that rules on content moderation might further aggravate the already intense monitoring of individuals behaviour online. In this regard, it advocated for express language on the fact that content moderation must not consist in *"the monitoring or profiling of the behaviours of individuals, unless the provider can demonstrate, on the basis of a risk assessment, that such measures are strictly necessary to mitigate the categories of systemic risks identified in Article 26"*.[76]

The amendments proposed in the JURI opinion introduce an exceptional extension of the notice and action procedure set out in the Commission's proposal. Under the JURI's Article 14(1), providers of instant messaging services (used for non-private or commercial purposes) and hosting services are required to make available tools to notify content which is either illegal or "in breach of their terms and conditions".[77] Furthermore, the same article introduce a 72-hours deadline for the service providers to process the notices and remove or deactivate access to the content at issue. The JURI's notice and action mechanism, characterized by very short timeframes and an extension of the procedure to more providers (such as instant messaging services) and to more content (that which is allegedly in contrast with terms and conditions),

[75] EDPS Opinion on the DSA, p. 12.
[76] Ibid., p. 13.
[77] JURI Committee opinion on the DSA, Article 14 (1).

appears extremely problematic from a fundamental rights perspective. The proposed system clearly forces providers to use (even more) filters, including to prevent the re-upload of previously removed content. This brings about the risk that service providers over-remove perfectly legal content, without ever ascertaining the illegal nature of a specific piece of content.

2.4.4. Additional provisions applicable to online platforms

2.4.4.1. Internal complaint-handling (Article 17) and out-of-court dispute settlement (Article 18)

The DSA proposal sets out a series of procedural obligations on the management of disputes which might arise between online platforms and users. Such disputes may concern the platforms' decisions to remove content posted by the user, or to suspend or terminate the provision of the service to users or their account, based of the alleged illegality of content or its incompatibility with platforms' terms and conditions.[78] Online platforms must enable users to challenge such decisions through an internal complaint-handling system, electronic, free of charge and not solely relying on automated means. Decisions must be reversed without undue delay where the complaint offers "sufficient grounds" to determine that the content at issue is not illegal or incompatible with the terms and conditions.[79]

Furthermore, Article 18 DSA proposal introduces an additional potential remedy for those users who received a decision consisting in access removal, suspension or termination of the service. These users are entitled to file a complaint before any certified out-of-court dispute settlement body[80] which has been authorized by the DSC to solve these types of disputes. The DSA proposal specifies that bringing the dispute to one of these extra-judicial settlement bodies, which (among other conditions) must be independent from platforms and users, does not impact the possibility to proceed with an action through the normal court system.

According to Article 18(3), where the dispute is decided in favour of the user, the platform must reimburse any fees and other reasonable expenses. On the contrary, if the platform wins the dispute, the user will not be required to reimburse the platform of such cost. However, users will still bear their own costs to challenge the decision before a settlement body. While this rule can act as a deterrent to ungrounded claims, it may still discourage users from undertaking such an initiative depending on the costs of engagement of the dispute settlement body.

[78] Article 17(1) DSA proposal.
[79] Article 17(3) DSA proposal.
[80] Conditions for certification are listed under art. 18(2) DSA.

The industry argued that access to the out-of-court settlement procedure should be made conditional upon the exhaustion of the internal complaint procedure.[81] However, in light of the fundamental right issues at stake, it seems reasonable to consider that the recipients of a decision should be capable of bringing their claims directly before the out-of-court settlement body.

2.4.4.2. Trusted flaggers (Article 19)

An important feature of the DSA proposal's codification of notice and action procedures consists in the creation of the category of "trusted flaggers". Upon application, any entity can in principle be granted this status by the relevant Digital Services Coordinator (DSC). Therefore, the nature and mission of trusted flaggers can vary significantly, ranging from law enforcement units, to NGOs, to organizations of industry and right-holders, etc (recital 46). To be accredited, entities must meet a series of cumulative conditions listed under Article 19(2) DSA:

a) particular expertise and competence in detecting, identifying and notifying illegal content;
b) representation of collective interests and independence from any online platform;
c) submission of notices in a timely, diligent and objective manner.

Article 19 DSA requires online platforms to process notices submitted by trusted flaggers pursuant to the notice and action mechanism "with priority and without delay".[82] As the DSA confers a privileged status to the trusted flaggers' notifications, their (un)trustworthiness raises significant issues. A particularly sensitive question relates to the possibility that law enforcement agencies could become trusted flaggers, and then be able, in that capacity, to send informal notices instead of a legal order. The rights and interests at stake suggest that a proper legal process should govern law enforcement-driven removals.

The proposal also defines a procedure to scrutinize failures of the trusted flaggers in carrying out their activities, which can potentially result in the withdrawal of their accreditation. Specifically, when a platform considers that a trusted flagger submitted "a significant number of insufficiently precise or inadequately substantiated notices", it must refer the relevant information to the competent regulator, providing explanations and details.[83] Following an investigation, the DSC may revoke the accreditation after having given the entity "an opportunity to react" to its findings and decision.[84]

The meaning of "insufficiently precise or inadequately substantiated notices" is currently unclear. Considering the implications of the activity of untrustworthy trusted flaggers, the

[81] DIGITALEUROPE, position paper on DSA, p. 10.
[82] Article 19(1) DSA proposal.
[83] Article 19(5) DSA proposal.
[84] Article 19(6) DSA proposal.

proposal could be more specific on this concept. Article 19(6) now entirely refers its interpretation to future guidance possibly issued by the Commission.

The proposal does not allow platforms to appoint their "trusted flaggers", a choice that is opposed by the industry, which argues that platforms should be free to choose their own trusted flaggers[85]. However, platforms still hold considerable power as they are in the "driver seat" when it comes to deciding to refer an "untrustworthy" flagger to the DSC and providing the DSC with the information that will support its investigation.

The JURI Committee opinion on the DSA significantly intensifies the pressure to deal with the notifications submitted by trusted flaggers, as it requires online platforms and hosting services to "immediately" process such notifications.[86] In the JURI's amendments, trusted flaggers can also represent individual right holders and must be independent not only from the platforms but also from "law enforcement, or other government or relevant commercial entity".[87] Moreover, trusted flaggers recognized in a certain Member State can be awarded the same status by the authorities of another Member State, and promoted to European trusted flagger by the Board.[88]

2.4.4.3. Measures and protection against misuse (Article 20)

The proposal sets out rules to be adopted by the platforms against the misuse of the services and of the notice and action procedure. Specifically, Article 20 DSA requires platforms to suspend, "for a reasonable period of time and after having issued a prior warning":

i) the provision of services to those users who "frequently provide manifestly illegal content";
ii) the processing of notices and complaints by subjects that "frequently submit notices or complaints that are manifestly unfounded".

Online platforms are required to define the policy *vis à vis* these types of misuses in their terms and conditions, together with the main circumstances taken into consideration to determine a misuse. Such circumstances include the elements listed under Article 20(3), such as the proportion between the total number of items provided or notices submitted and those which have been found to be manifestly illegal or unfounded.

The proposal, however, is not specific on the meaning of crucial concepts such as "manifestly illegal" or "frequently" or on how platform should, in their position, perform an evaluation of the (complex) circumstances listed under Article 20(3) (such as, for instance, the "intention" of the user).

[85] DIGITALEUROPE, position paper on DSA p. 11.
[86] JURI Committee opinion on the DSA, new Article 14a, paragraph 1.
[87] Ibid., paragraph 2.
[88] Ibid., paragraph 3a.

The language of Article 20 seem to exclude permanent suspension and suspension after a single episode; however, the terms of service of the platforms could be stricter than Article 20 and provide for these types of measures against misuse.

2.4.4.4. Notifications of suspicions of criminal offences (Article 21)

Article 21 establishes a duty for online platforms to promptly inform the law enforcement or judicial authorities of the Member State(s) concerned when they "[become] aware of any information giving rise to a suspicion that a serious criminal offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place". The proposal expressly clarifies that it does not intend to provide platforms with a legal basis to profile users "with a view to the possible identification of criminal offences".

Article 21 imposes on the platforms very significant obligations in terms of cooperation and information-sharing with law enforcement. The scope of the information shared with law enforcement may be very broad ("any information giving rise to a suspicion" of a current or potential criminal offence) which raises concerns of due process and procedural safeguards Related to this, and recalling the principle of legal certainty, the EDPS recommended that the co-legislators specify which criminal offences (other than child sexual abuse, mentioned by recital 48) trigger the notification obligation and define more precisely what constitutes "relevant information".[89] With regard to the categories of offences subject to notification, BEUC supported extending the reporting obligation to illegal activities such as fraudulent ads and the sale of illegal products.[90]

2.4.4.5. Traceability of traders (Article 22)

Article 22 DSA introduces in the proposal a "Know Your Business Customer" principle ("KYBC") with a view to go beyond the (often ignored and unenforced) information requirements of Article 5 e-Commerce directive.[91] In particular, the proposal requires platforms intermediating between consumers and traders to make the use of their services by traders conditional upon the acquisition of the information to identify them (such as details of the trader, details of the economic operator, register number in the trade register and a self-certification of the trader about compliance with the relevant EU rules). Platforms must dedicate reasonable efforts in verifying whether such information is reliable; moreover, they must suspend traders where they "obtain indications that any item of information […] is inaccurate or incomplete" and traders fail to correct such information.

According to BEUC, the text must be amended to clarify that only legitimate traders can be allowed on the platforms and to introduce an obligation for platforms to carry out regular

[89] EDPS opinion on the DSA, p. 14.
[90] BEUC position paper on the DSA, p. 23-24.
[91] https://www.kybc.eu/wp-content/uploads/2020/10/KYBC_letter_29102020.pdf

checks on the traders' legitimacy and on the information these provide.[92] Moreover, the obligation to perform controls on a rolling basis should also involve existing traders and operate regardless of a specific suspicion that the information is incomplete or inaccurate.[93]

Other aspects which are left unclear under the current proposal concern the possible liability of the platforms for traders' information which turns out to be false[94] and their liability *vis à vis* consumers for failure to comply with the obligations under article 22.[95] Following the publication of the proposal, doubts have been voiced about the capability of the KYBC rules to tackle the sale of illegal products. In particular, the lead rapporteur for the European Parliament IMCO Committee declared that the proposal does not go far enough in ensuring safety of online marketplaces and that appropriate amendments (including a possible "importer responsibility" clause) were being considered in this regard.[96]

With a view to increase protection for consumers, the draft IMCO opinion published in May 2021 significantly extends the scope of the identification obligations set out under Article 22 of the original DSA proposal. The rules on traceability apply not only to online marketplaces, but to all information society services, and are not limited to traders, but extend to products and services.[97] Moreover, when a relevant authority informs the online platform that an offer for a product or a service is illegal under EU or national law, the platform must remove the offer and inform the trader according to Articles 15 and 17 DSA proposal.[98]

2.4.4.6. Transparency reporting obligations for providers of online platforms (Article 23)

Online platforms are subject to transparency reporting obligations which apply in addition to the ones set forth for all providers of intermediary services in Article 13. Specifically, they must publish, every six months, data on their average monthly users in each Member State and also include, in the yearly transparency reports referred to in Article 13, information on the following:

a) the number of disputes referred to the out-of-court dispute settlement bodies, their outcomes and the average length of those procedures;
b) the "number of suspensions imposed pursuant to Article 20", distinguishing between the grounds for the suspension;

[92] BEUC position paper on the DSA, p. 24-25.
[93] Ibid.
[94] DIGITALEUROPE position paper on the DSA, p. 12.
[95] BEUC position paper on the DSA, p. 25.
[96] Stolton, S., *MEP vies to target rogue traders in Digital Services Act*, Euractiv, Febrary 2021, available at : https://www.euractiv.com/section/digital/news/mep-vies-to-target-rogue-traders-in-digital-services-act/
[97] IMCO Committee draft report on the DSA, Article 13(b) new.
[98] Ibid., Article 22.

c) "any use made of automatic means for the purpose of content moderation", indicating their precise purposes, data about the accuracy of the automated means in achieving such purposes and possible safeguards applied to the process.

In addition to these, further transparency reporting obligations apply to VLOPs, which are detailed under Article 33.

2.4.4.7. Online advertising transparency (Article 24 and Article 30)

The DSA proposal introduces a set of ad transparency obligations for the platforms displaying advertising on their online interfaces. Pursuant to Article 24, platforms are required to provide users with specific information on the advertisements they visualize, "in a clear and unambiguous manner and in real time". In particular, users must be provided with the following information:

a) that the information displayed amounts to an advertisement;
b) "the natural or legal person on whose behalf the advertisement is displayed";
c) "meaningful information about the main parameters" applied to determine the users to whom the advertisement is shown.

Article 30 of the proposal envisages additional ad transparency obligations for the VLOPs[99], requiring them to establish and make available to the public via APIs a repository of the information relating to a specific ad.[100] The repository, which must be publicly available until one year after the last appearance of the ad on the platforms, must include at least the following elements:

a) "the content of the advertisement;"
b) "the natural or legal person on whose behalf the advertisement is displayed";
c) "the period during which the advertisement was displayed";
d) whether one or more particular groups of users were the intended target of that advertisement "and if so, the main parameters applied to achieve the targeted display of the ad";
e) the total number of users of the platform reached and, "where applicable, aggregate numbers for the group or groups of users to whom the advertisement was targeted specifically".

In October 2020, the European Parliament adopted three resolutions on the DSA[101]. As explained in part I of this paper, the resolutions of the European Parliament called on the

[99] The DSA provisions applicable to VLOPs are discussed in the following section of this paper.
[100] For a discussion, see Leerssen P., *Platform Ad Archives in Article 30 DSA*, available at: https://dsa-observatory.eu/2021/05/25/platform-ad-archives-in-article-30-dsa/
[101] European Parliament, Resolution on improving the functioning of the Single Market (2020/2018(INL)); European Parliament, Resolution on adapting commercial and civil law rules for commercial entities operating

Commission to introduce stricter rules on targeted advertising - the core business model underpinning online platforms - and, specifically, invited the Commission to consider "a phasing out, leading to a prohibition" of targeted advertisement.[102]

The DSA proposal, however, limits itself to a basic transparency-based approach. The draft regulation does not provide any express explanation on this policy choice. It can be assumed that the Commission considered that the issues connected to the processing of personal data for advertising purposes (including the distortions of business models relying on a rather unlimited collection of personal data) should be addressed through the application of the GDPR and the upcoming e-Privacy Regulation. Moreover, the Commission's assumption that smaller businesses would be affected by the transition to a different advertising model might have also played a role in shaping the DSA's rules on online advertising. While this idea is defended with great conviction by the relevant platforms,[103] recent studies cast major doubts on the effectiveness of this advertising model and conclude that less privacy-intrusive advertising schemes can actually bring more opportunities for both advertisers and publishers (with less money spent in middlemen). [104]

Most of the position papers issued after the presentation of the DSA proposal - notably, by the EDPS and civil society organizations including BEUC, EDRI, Amnesty International[105] - expressed concerns about the approach opted for by the Commission in tackling the serious risks associated with targeted advertising and recommended the introduction of rules going beyond transparency. Reaction to the ads-related provisions in the DSA proposal has also prompted MEPs-level initiatives such as the "Tracking Free Ads Coalition".[106]

It can be safely argued that policy initiatives aiming at stronger restrictions of the platforms' surveillance-based business model would have a very strong democratic backing. For instance, since the release, at the end of April 2021, of Apple's iOS 14.5, which requires apps to ask users permission to track them and allows turning-off app tracking entirely, only 4% of users opted-in.[107] These opt-in rates allow for a rather simple yet unequivocal conclusion, which should be duly considered in the evidence-based policy-making pursued by the EU. When

online (2020/2019(INL)); European Parliament, Resolution on the Digital Services Act and fundamental rights issues posed (2020/2022(INI)).

[102] Resolution on adapting commercial and civil rules (2020/2019(INL)), para 15 and 17; Resolution on improving the functioning of the Single Market (2020/2018(INL)), p. 26.

[103] See, for instance: https://about.facebook.com/actions/europe

[104] Iwańska K., *To track or not to track? Towards privacy-friendly and sustainable online advertising*, Panoptikon Foundation, 2020; for an overview on the economics of online publishing and successful experiences of sustainable (no-tracking based) publishing, see: Irish Council for Civil Liberties, *Sustainable without surveillance*, 2021, available at: https://www.iccl.ie/wp-content/uploads/2021/10/Sustainable-without-surveillance.pdf.

[105] Amnesty International, *Position on the Proposal for a Digital Services Act and a Markets Act*, available at: https://www.amnesty.eu/news/amnesty-international-position-on-the-proposals-for-a-digital-services-act-and-a-digital-markets-act/

[106] https://trackingfreeads.eu/; Lomas, N., *Inside a European push to outlaw creepy ads*, Techcrunch, 21 October 2021, available at: https://techcrunch.com/2021/10/21/inside-a-european-push-to-outlaw-creepy-ads/

[107] https://mashable.com/article/ios-14-5-users-opt-out-of-ad-tracking/?europe=true. The data available refers to the rate of opt-in registered in the United States, but it can be assumed that the rate of opt-ins in the EU would be following similar trends.

given a real choice, the overwhelming majority of the population chooses not to be subject to online tracking and not to trade their privacy (and other fundamental rights) for some more targeted advertising.

The EDPS expressed strong support for the European Parliament's resolutions and urged the co-legislators "to consider a phase-out leading to a prohibition of targeted advertising on the basis of pervasive tracking"[108]. Moreover, the EDPS suggested introducing additional limitations to the processing of data for targeting purposes, which should restrict the following:[109]

a) "categories of data that can be processed for targeting purposes" (with the exclusion of off-platform tracking);
b) categories of data or criteria (such as those directly or indirectly involving special categories of data) used to deliver targeted advertising;
c) "categories of data that may be disclosed to advertisers or third parties" in the targeting process.

The current Articles 24 and 30 of the proposal, by requiring platforms to provide "meaningful information about the main parameters", will leave substantially unprejudiced the transparency features currently offered by the main platforms, where ads delivered on the basis of pervasive (including off-platform) tracking are explained with extremely generic parameters. [110] These loose targeting parameters (for instance, woman aged 25-55; speaking English; resident in the Netherlands) appear to fall short of meaningful transparency, as they mask the much more granular profiling and pervasive analytics that enabled the targeting of very particular demographics or even a specific user with a specific ad.

In addition, the approach opted for by the Commission as regards advertising seems to be lacking empirical evidence about the effectiveness of the proposed transparency rules. In fact, recent empirical research has revealed that transparency labels (such as sponsorship disclosures on digital political advertisements) go unnoticed by users and have very limited effects.[111]

As explained in the IMCO Committee draft report, there is a good case to be made for imposing stricter rules - in line with the previous IMCO INL report adopted in October 2020 - to limit the pervasive processing of personal data which enables the delivery of targeted advertsing.

First, the IMCO (draft) report replaces Article 24 DSA proposal with a new provision which extends online advertising transparency rules well beyond online platforms, to reach all intermediary services. In addition to the information to be provided under Article 24 of the

[108] EDPS opinion on DSA, p. 15-16.
[109] EDPS opinion on the DSA, paragraph 70.
[110] Amnesty International position paper on the DSA, p. 8; BEUC position paper on the DSA, p. 25.
[111] Dobber, T. et al, *Effectiveness of online political ad disclosure labels: empirical findings*, 2021, available at: https://www.uva-icds.net/wp-content/uploads/2021/03/Summary-transparency-discloures-experiment_update.pdf

Commission proposal, the IMCO draft requires intermediaries to specify whether the advertisement was placed through an automated tool and "the identity of the person responsible for that tool".[112] Moreover, researchers, NGOs and public authorities must be given "easy access" to information concerning "direct and indirect payments or any other remuneration received" to show the advertisement on their pages.

Second, and crucially, the IMCO draft report mandates that, by default, users cannot be subject to "targeted, microtargeted and behavioural advertisement" unless their "freely given, specific, informed and unambiguous consent" has been collected for theses purposes. In any case, even when processing data to deliver targeted, micro-targeted and behavioural advertising, intermediaries must refrain from pervasive tracking, "such as disproportionate combination of data collected by platforms, or disproportionate processing of special categories of data that might be used to exploit vulnerabilities".[113]

With specific regard to the obligation under Article 30(2)(d), concerning groups of users identified as the intended targeted of an ad, the EDPS recommended that all exclusion criteria should also be reported in the repository to allow for the identification of unfair or discriminatory patters.[114] The IMCO report follows this recommendation and introduces an obligation for the VLOPs to indicate whether groups of users "have been explicitly excluded from the advertisement target group".[115]

2.5. Additional obligations for very large online platforms to manage systemic risks

The DSA establishes additional obligations for those platforms which qualify as VLOPs, for having a number of average monthly active users in the Union equal to or higher than 45 million. Every six months, the DSC of establishment will verify whether the platforms under their jurisdiction meet (or no longer meet) the parameters to be designated as VLOP.

In reaction to the DSA proposal, BEUC argued that the threshold established for the VLOP definition to apply (45 million monthly active users) is too high, while the concept of "active" is also very unclear. Indeed, the current parameters would only tackle very few platforms and leave most of the major platforms analyzed by the EC in the impact assessment exempted from all the core VLOPs' obligations, relating to systemic risk assessment and mitigation.[116] The IMCO Committee draft report introduced a significant amendment on the criteria set out by Article 25 to identify VLOPs, with the stated goal of ensuring that online marketplaces are brought within the scope of Section IV DSA proposal.[117] Specifically, an online platform will qualify as VLOP either when having a number of average monthly users equal to or higher

[112] IMCO Committee draft report on the DSA, Article 13 (c).
[113] Ibid., Article 13 (d).
[114] EDPS opinion on DSA, p. 15.
[115] IMCO Committee draft report on the DSA, Article 30(2), new point (ea).
[116] BEUC position paper on the DSA, p. 16.
[117] IMCO Committee draft report on the DSA, Article 25.

than 45 million, or when having "an annual turnover exceeding EUR 50 million within the EU".[118]
While the European Parliament's LIBE Committee opinion on the DSA, adopted in July 2021,[119] does not amend the VLOPs definition and relevant parameters, the JURI opinion introduces a major extension in the scope of application of Section IV Chapter III DSA (Additional obligations for VLOPs), mandating that "live streaming platforms, instant messaging services used for purposes other than private or non-commercial and search engines" are also subject to the systemic risks management obligations imposed on VLOPs.[120]

This section provides a critical overview of the obligations set out by the DSA for VLOPs. The additional VLOPs' obligations on advertising (provided for by Article 30) have already been addressed under Article 24, as analogous considerations apply to both provisions.

2.5.1. Risk assessment (Article 26) and mitigation of risks (Article 27)

Articles 26 and 27 on systemic risk assessment and mitigation, together with Article 28 on independent audits (commented below), constitute the core provisions of the "risk governance" model underpinning the DSA proposal. This is the model which has been opted for by the Commission to address the multifaceted risks and harms associated with the services and quality of content moderation by dominant platforms. Acknowledging the societal concerns caused by an advertising-driven business model which is common for most dominant services qualifying as VLOPs, recital 56 of the DSA proposal explains that "[i]n the absence of effective regulation and enforcement, [VLOPs] can set the rules of the game, without effectively identifying and mitigating the risks and the societal and economic harm they can cause".
Given the importance of these provisions, the description of the rules set out under Articles 26 and 27 is followed by a more detailed analysis of the possible aspects of inconsistency and ineffectiveness of the current draft, including, where possible, suggestions for amendments.

Pursuant to Article 26, VLOPs are required to "identify, analyse and assess, at least once a year, any significant systemic risks stemming from the *functioning and use* made of their services in the Union". Specifically, Article 26(1) provides that the assessment must consider the following systemic risks in connection with the specific services (emphasis added):

a) "the dissemination of *illegal content* through their services;
b) any *negative effects for the exercise of the fundamental rights* to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child, as enshrined in Articles 7, 11, 21 and 24 of the Charter respectively;

[118] Ibid.
[119] Opinion of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) for the Committee on the Internal Market and Consumer Protection (IMCO) on the DSA proposal, 28 July 2021, available at: https://www.europarl.europa.eu/doceo/document/LIBE-AD-692898_EN.pdf
[120] JURI Committee opinion on the DSA, Amendment 263 and Article 25.

c) *intentional manipulation* of their service, including by means of inauthentic use or automated exploitation of the service, with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security".

In the context of their risk assessments, Article 26(2) would require VLOPs to consider how the systemic risks identified above are impacted by "their content moderation systems, recommender systems and systems for displaying advertisement",[121] having regard also to the "potentially rapid and wide dissemination" of content which is illegal or in violation of their terms and conditions.

Once systemic risks have been identified, VLOPs must implement "reasonable, proportionate and effective mitigation measures" to address those risks (Article 27). Such measures may include:

a) "adapting content moderation or recommender systems, their decision-making processes, the features or functioning of their services, or their terms and conditions;
b) targeted measures aimed at limiting the display of advertisements in association with the service they provide;
c) reinforcing the internal processes or supervision of any of their activities in particular as regards detection of systemic risk;
d) initiating or adjusting cooperation with trusted flaggers in accordance with Article 19;
e) initiating or adjusting cooperation with other online platforms through the codes of conduct and the crisis protocols referred to in Article 35 and 37 respectively."

The main systemic risks identified by VLOPs or through other sources (for instance, vetted researchers pursuant to Article 31) are included in a yearly report issued by the Board - the advisory group composed of the Digital Services Coordinators (DSCs) - alongside best practices to mitigate the systemic risks identified.
VLOPs' compliance with the due diligence obligations set out in Chapter III DSA (including risk assessment and mitigation) must be assessed yearly by an independent auditor (Article 28 commented in the paragraph below).

Articles 26 and 27 are the cornerstone of the risk management approach introduced by the DSA proposal. By establishing a connection between VLOPs' operations and a series of possible systemic risks, and by requiring VLOPs to identify and mitigate such risks, these rules represent a significant advancement in EU platform regulation. However, at a closer look, the current wording of Articles 26 and 27 appears vague and potentially problematic on a number of aspects, which raise doubts about the ability of the whole risk assessment and mitigation infrastructure to deliver meaningful accountability *vis à vis* dominant online services.

[121] Article 26(2), DSA proposal.

Crucially, the proposed assessment and mitigation obligations pose concerns about their possible impact on fundamental rights, and in particular freedom of expression.

The main concerns about the DSA's systemic risks provisions revolve around the uncertain scope of Article 26(1) on risk assessment and Article 27 on risk mitigation, which directly impact the scope and effectiveness of a number of other DSA provisions (including the rules on oversight and enforcement). In the first place, the "selective" risk list under Article 26(1) restricts the reach of Article 26(2), which mandates platforms to consider how the systemic risks of Article 26(1) are affected by their content moderation, recommender and advertising systems. Another example of a provision impacted by the scope of Article 26(1) is Article 31 on data access and scrutiny, which provides that vetted researchers can be granted access "for the sole purpose of conducting research contributing to the identification and understanding of systemic risks as set out in article 26(1)".

i. Dissemination of illegal content through VLOP's services

As noted by Barata, illegal content is understood by Article 26(1)(a) "not only as a broad category, but as something that needs to be assessed by VLOPs in bulk".[122] Significant issues in the implementation of this obligation (and the related risk mitigation) arise first and foremost from the fact that most of the alleged illegal content will simply be removed on the basis of notice and takedown procedures, without ever being determined illegal as a result of a more extended legal assessment.
The LIBE Committee opinion on the DSA specifies the scope of the impact assessment on illegal content, stating that it must concern manifestly illegal content or content which has been the subject of an order under Article 8 DSA proposal.[123]

ii. Negative effects on fundamental rights

The reference of Article 26(1)(b) to "any negative effect" appears rather broad and difficult to implement in practice, especially because no specifications are included on how to give account of, and assess, the areas of tension between different fundamental rights which need to be mutually balanced.[124]

Article 26(1)(b)lists a series of four fundamental rights which might be impacted by the functioning and use of the VLOPs' services: the right to privacy, freedom of expression and information, the rights of the child and the prohibition of discrimination. However, it is unclear

[122] Barata J., *The Digital Services Act and its impact on the right to freedom of expression: special focus on risk mitigation obligations*, Plataforma por la Libertad de Información, available at: https://libertadinformacion.cc/wp-content/uploads/2021/06/DSA-AND-ITS-IMPACT-ON-FREEDOM-OF-EXPRESSION-JOAN-BARATA-PDLI.pdf. Barata also observes that the term "illegal content" seems to refer both to content that has already been declared illegal or treated as illegal under the DSA and to (not yet existing) illegal content which is likely to be produced and disseminated.
[123] LIBE Committee opinion on the DSA, Article 26(1)(a).
[124] Barata J., *The Digital Services Act and its impact on the right to freedom of expression: special focus on risk mitigation obligations*, p. 18.

why the risk assessment and mitigation should be limited to these four fundamental rights and disregard the threats posed to other fundamental rights and freedoms enshrined in the EU Charter of Fundamental Rights (and protected in human rights instruments in Europe and internationally). In fact, there is little doubt that fundamental rights such as the right to health (including mental health), dignity, integrity of the person and the protection of personal data, together with many others, including social and cultural rights, might very well be affected by the VLOPs' services.

Furthermore, the current language of Article 26(1)(b) is in contrast with recital 57, according to which the list is not exhaustive. Indeed recital 57 explains that the "second category concerns the impact of the service on the exercise of fundamental rights, as protected by the Charter of Fundamental Rights, *including* the freedom of expression and information, the right to private life, the right to non-discrimination and the rights of the child". According to Amnesty International - which recalls the recent European Commissions' Sustainable Corporate Governance Initiative, introducing rules on mandatory corporate environmental and human rights due diligence - the obligations under Article 26 *"must go further and extend to compulsory and effective human rights due diligence requiring the VLOPs' to identify, cease, prevent, mitigate, monitor and account for their impacts on any human rights, in line with international standards including the UN Guiding Principles on Business and Human Rights"*.[125]

The LIBE report broadens the scope of the impact assessment on fundamental rights, requiring VLOPs to consider any negative effect on fundamental rights, focusing "in particular" on the fundamental rights listed under the Commission's proposal as well as on the protection of personal data and the freedom of the press.[126] The IMCO report applies a similar extension to the scope of Article 26(1)(b), where all negative effects for fundamental rights are relevant to the assessment, with a particular attention for the fundamental rights indicated by the original proposal and, additionally, "consumer protection".[127]

iii. <u>Intentional manipulation of the services</u>

Article 26(1)(c) focuses exclusively on how services are *intentionally manipulated* and therefore it excludes from the assessment those systemic risks which are posed by the *normal* design, functioning and use of the VLOPs services. A systemic risk of societal harm which would be disregarded under article 26(1)(c) is, for instance, the risk stemming from the internal systems of the VLOP which are designed (i.e., intended to) to maximize engagement and ads-revenues and that, as such, end up favouring the spread of divisive content and increasing polarization. Analogous concerns have been raised by the EDPS, which underlined in its

[125] Amnesty International position paper on the DSA, p. 10.
[126] LIBE Committee opinion on the DSA, Article 26(1)(b).
[127] IMCO Committee opinion on the DSA, Article 26(1)(b).

opinion on the DSA that systemic risks can derive from the services of VLOPs "independently of whether they are manipulated or not".[128]

In addition to the issues listed above, the current scope of Article 26(1), which identifies the "functioning and use made of [the VLOPs'] services" as subject matter of the systemic risk assessment, might also be too narrow. As such, this provision would likely be unable to capture systemic risks comprehensively and effectively. This is particularly the case in the absence of a stricter regulation of the platforms' business model through the introduction of restrictions on targeted advertising. Thus, Article 26 could perhaps include specific language on the fact that it is not just the "functioning and use made of the services" to potentially pose systemic risks, but also their design and the development of existing services as well the creation of new ones. For instance, Facebook's announced project of creating an Instagram service for kids under the age of thirteen[129] is a relevant example of the systemic risks associated with the development by platforms of new services and/or evolution of existing ones. These recent developments further show that, to achieve meaningful risk identification, prevention and mitigation, new services under development should be scrutinized through the risk assessment and mitigation procedure before being deployed.
Notably, the LIBE report extends the scope of the impact assessment under Article 26 to this crucial aspect, requiring VLOPs to conduct such assessment "always before launching new services", analysing "the probability and severity of any adverse impact of the design, functioning and use made of their services in the Union, in particular on fundamental rights, including any systemic impact at the level of a Member State".[130]

Article 27 requires VLOPs to implement "reasonable, proportionate and effective" mitigation measures *vis à vis* the systemic risks identified under Article 26. Several position papers have evaluated the scope of the VLOPs' obligation under Article 27 as narrow and unambitious for being limited to the implementation of mere "mitigation measures", i.e., for not envisaging any duty for the VLOPs to adopt measures to *prevent, eliminate* (where possible) and in any case *minimize* the systemic risks (as usually is the case in the context of risk management). The call for stricter obligations is understandable, especially where systemic risks of individual and societal harms are inherent to the functioning and use of the VLOPs services.
However, it must be also considered that such stricter obligations could be problematic from a freedom of expression standpoint, particularly to the extent they translate in the adoption of proactive measures.

2.5.2. Independent audit (Article 28)

Article 28 on independent audits provides that VLOPs must conduct audits on a yearly basis to assess their level of compliance with the obligations set out in Chapter III of the DSA as well

[128] EDPS opinion on the DSA, p. 18.
[129] https://www.cnbc.com/2021/05/10/attorneys-general-ask-facebook-to-abandon-instagram-for-kids-plans.html
[130] LIBE Committee opinion on the DSA, Article 26(1).

as with the codes of conduct referred to in Articles 35 and 36 and the crisis protocols under Article 37.

The audit reports must indicate the specific elements subject to audit, the methodology adopted and the main conclusions from the audit.[131] An audit opinion has to be provided in the report on whether the audited VLOP complied with the abovementioned obligations and commitments. Where the audit opinion is negative (or positive with comments), the auditor must provide operational recommendations on specific measures to achieve compliance.[132] These recommendations must be followed in one month by an audit implementation report where the VLOP outlines the envisaged corrective measures and explains the reasons for not implementing certain recommendations.[133]

Under Article 28, auditors are required to verify the compliance of VLOPs with their due diligence obligations. Among these obligations, systemic risks identification and assessment and mitigation measures stand out as the pillars of the regulatory structure applicable to VLOPs. However, Article 28 does not require auditors to (re)assess the VLOP's risk assessment and to carry out their own investigation on such possible risks. What seems to be expected from an auditing firm, under the current draft, is to verify that the VLOP has complied with the obligation to perform a risk assessment and that the mitigation measures identified by the VLOP are coherent with its own findings about the systemic risks posed by its own services. Given the limited time and (human and technical) resources available to perform their tasks, the firm contracted for the audit will invariably have to rely on the information provided by the VLOP (which inevitably affects the effectiveness and independent character of the verification carried out).

It is questionable whether this would be enough to achieve an effective identification and mitigation of the risks associated with the VLOPs' operations. To ensure that possible flaws in the risk assessment conducted by the VLOPs are detected and that all additional systemic risks are identified (and, consequently, subject to appropriate corrective measures), a specific obligation would need to be imposed on auditors to conduct – themselves - an assessment of the systemic risks. In light of these considerations, the audit mechanism should be duly reassessed by the co-legislators, especially because this mechanism is a crucial tool put in place by the DSA to scrutinize the conduct of the VLOPs in relation to the systemic risks stemming from their very operations.

While the IMCO Committee draft report does not include any amendment on Article 28, the LIBE Committee report put significant emphasis on the elements of independence of the audit and on its crucial subject matter: "the identification, analysis and assessment of the adverse impacts referred to in Article 26, and the necessity, proportionality and effectiveness of the impact mitigation measures referred to in Article

[131] Article 28(3) DSA proposal.
[132] Ibid.
[133] Ibid., paragraph 4.

27".[134] The LIBE report prescribes that auditors have to be independent, with no conflict of interest with the audited platform or other VLOPs. All relevant information has to be shared with the auditors, which are required to give account of the elements on which a conclusion could not be reached (explaining "why these elements could not be conclusively audited"), and describe the third-parties consulted as part of the audit.[135]

2.5.3. Recommender systems (Article 29)

Article 29 DSA requires VLOPs to explain in their terms and conditions the "main parameters" which govern their recommender systems.[136] VLOPs must also indicate the options - if any - made available to the users "to modify or influence those main parameters, including at least one option which is not based on profiling".[137] Where users are offered a variety of options, the VLOPs' interface must enable them to change at any time their preferences for each of the recommender systems governing the curation of content, specifically with regard to the "relative order of information presented to them".[138]

The DSA acknowledges the specific role that recommender systems exert on the ability of users to interact with information as well as their impact in "the amplification of certain messages, the viral dissemination of information and the stimulation of online behaviour" (recital 62). As Helberger et al. have noted, however, the current wording of Article 29 fails to fully act upon this premise and to empower users with meaningful levels of transparency and control. [139] Notably, the DSA does not make it mandatory for VLOPs to provide users with control over how recommenders influence the display of information. As explained by recital 62, they "should ensure that the recipient enjoy alternative options", but the design and adoption of such alternatives rests upon the mere discretion of the VLOP.

The vague reference to the "main parameters" also appears problematic from several perspectives. First, it makes the content of this obligation quite narrow and enables platforms to reach compliance with a very superficial level of disclosure to users of how their content is curated. Second, the terms and conditions - detailed documents covering all aspects of the user-platform contractual relationship - are probably not the most appropriate setting to inform the user in a "clear, accessible and easily comprehensible manner". Third, as pointed out by Helberger et al., the "main parameters" are also difficult to identify from a technical perspective, as "[i]n most state-of-the-art recommender systems, which are usually some form

[134] LIBE Committee opinion on the DSA, Article 28.
[135] Ibid.
[136] Article 29(1) DSA proposal.
[137] Ibid.
[138] Article 29(2) DSA proposal.
[139] Helberger, N., Van Drunen, M., Vrijenhoek S., Möller, J., *Regulation of news recommenders in the Digital Services Act: empowering David against the Very Large Online Goliath*, Internet Policy Review, Opinion, 26 February 2021, available at: https://policyreview.info/articles/news/regulation-news-recommenders-digital-services-act-empowering-david-against-very-large

of machine learning model, it is not even entirely clear what the 'main parameters' in the model are and what their effects are".

The above considerations suggest that the rules envisaged under the current Article 29 are highly unlikely to provide users with meaningful transparency and control. As a consequence, in reaction to the proposal, the EDPS and several civil rights organizations converged on the following recommendations:

i. to replace the wording "main parameters" - as in the context of online ad transparency - with "parameters" or "all parameters" and in any case include clarifications as to what could amount to "meaningful information";[140]
ii. the option not based on profiling should be the default one, and profiling should only influence the systems where users have opted-in.[141]
iii. information on the recommender systems should not be incorporated in the already complex terms and conditions, but should be offered separately for increased transparency and control.

The IMCO Committee draft report picked up on some of these points of criticism and replaced Article 29 with a new Article 24(a) on Recommender Systems which applies not only to VLOPs but to online platforms as such.[142] Online platforms are required to activate by default the recommenders option not based on profiling, while profiling is subject to the user's "freely given, specific, informed and unambiguous consent". Users must be informed about the main parameters used in the recommender systems - including recommendation criteria, how these are balanced against each other; goals the system has been designed to achieve - as well as any options (including one not based on profiling) to modify these parameters.[143] Moreover, the draft report mandates online platforms to design the algorithm governing the recommender systems "in such a way that it does not risk misleading or manipulating" the users and requires them to prioritize public and scientific sources when it comes to "areas of public interest". [144]

2.5.4. Data access and scrutiny (Article 31)

Article 31 is one of the most innovative provisions of the DSA. Where the DSC of establishment or the Commission formulate "a reasoned request", VLOPs must provide them with access to data that are necessary to monitor and assess compliance with the DSA.[145] Furthermore, following again a "reasoned request" by the DSC or the Commission, VLOPs are required to grant access to data to vetted researchers "for the sole purpose of conducting

[140] EDPS opinion on the DSA, p. 17; BEUC position paper on the DSA, p. 26; Amnesty international position paper on the DSA, p. 12; EDRI position paper on the DSA.
[141] EDPS opinion on the DSA, p. 16-17.
[142] IMCO Committee draft report on the DSA, Article 24(a).
[143] Ibid.
[144] Ibid.
[145] Article 31(1) DSA proposal.

research that contributes to the identification and understanding of systemic risks as set out in Article 26(1)".[146]

In order to be "vetted" and qualify for access, researchers must meet a series of requirements:

i) affiliation with an academic institutions,
ii) independence from commercial interests,
iii) proven expertise in the area related to the risks investigated or related research methodologies,
iv) ability to keep the data secure and confidential as applicable. [147]

VLOPs can react to the access request demanding the DSC or the Commission to amend such requests on the basis of two motives:

a) their inability to satisfy the request because of lack of access to the data; or
b) granting access would result in significant vulnerabilities for the security of the service or for the confidentiality of information (particularly trade secrets).[148]

The introduction of a framework which compels VLOPs to provide access to data, with a view to enable scrutiny over their levels of compliance with the proposed Regulation and over the systemic risks which are posed by their services, is certainly to be welcomed.[149] However, the current formulation of Article 31 poses raises some questions about the capability of this provision to provide effective oversight and a mechanism "for bridging information asymmetries and establishing a resilient system of risk mitigation, informing online platforms, DSCs, other competent authorities, the Commission and the public".[150]

First, there is a tension between an access request under Article 31 and the protection of the companies' confidential information, in particular trade secrets. The scope of this derogation, and the way it plays out in practice, will directly impact the scope of the information which can be accessed under Article 31 and, in turn, the possibility to effectively map out and scrutinize the systemic risks associated with the platforms' activities. In light of these considerations, Article 31(7) could be more specific on what could constitute "alternative means" for access or "other data" where security or confidentiality concerns are raised to oppose an access request and demand its amendment.

[146] Article 26(2) DSA proposal.
[147] Article 31(4) DSA proposal.
[148] Article 31(6) DSA proposal.
[149] See also, Ausloos J., Leerssen P., Ten Thije, P., *Operationalizing Research Access in Platform Governance, What to learn from other industries?*, "Governing Platforms" AlgorithmWatch, available at: https://www.ivir.nl/publicaties/download/GoverningPlatforms_IViR_study_June2020-AlgorithmWatch-2020-06-24.pdf
[150] Recital 64 DSA proposal.

Article 31 should also clarify that, where researchers comply with the requirements listed under Article 31(4) to be vetted, the DSC and the Commission must forward the access request received from the researchers to the VLOPs. Moreover, it should be added that the Commission and the DSC must not engage in any assessment on the merit of the research and on whether it can be successful in analysing systemic risks.

Furthermore, as pointed out by Vermeulen, access to data should not be limited to academic researchers, but rather extended to scientific researchers.[151] While the DSA provides the platforms with a legal basis under GDPR to share data with researchers, the adoption of a code of conduct under art. 40 GDPR would be needed to ensure that data is shared in a GDPR-compliant way, including outside the specific DSA framework (i.e., without the "intermediation" of the Commission or of the DSC of the place of establishment).[152]

The IMCO draft report significantly broadens the scope of Article 31, by admitting researchers affiliated to civil society organizations among vetted researchers. Furthermore, the amendment proposed in the IMCO report introduces an obligations for the VLOPs to provide the DSC and the Commission with access to data "and algorithms" to monitor compliance with the DSA[153] and to "explain the design and the functioning of the algorithms" when asked to so by the DSC of establishment.[154]

One of the most notable amendments introduced by the IMCO report, related to scrutiny and risk assessment of the tools deployed by VLOPs, consists in a a new Article 33(a) on algorithmic accountability. The new provision requires VLOPs to provide the Commission with the information needed to assess their automated decision-making tools and the algorithms underpinning them. In carrying out its evaluation, which can benefit from the contribution provided by national authorities, researchers and NGOs, the Commission must assess the algorithms against a series of criteria. These include "the impact on fundamental rights, including consumer rights, as well as the social effects of the algorithms" and whether these elements are duly protected by the measures adopted by VLOPs to ensure the resilience of the algorithm at issue.[155]

2.5.5. Compliance officers (Article 32)

Very large online platforms shall appoint one or more compliance officers responsible for monitoring their compliance with this Regulation. These are tasked with cooperation with DSC establishment and Commission and with supervision of the activities connected with the independent audit.

[151] Vermeulen M., *The Keys to the Kingdom*, Kinght First Amendment Institute at Columbia University, available at https://knightcolumbia.org/content/the-keys-to-the-kingdom
[152] Ibid.
[153] IMCO Committee draft report on the DSA, Article 31.
[154] Ibid., Article 31 new paragraph 1(a).
[155] Ibid., new Article 33 (a).

2.5.6. Transparency reporting obligations for VLOPs (Article 33)

VLOPs must publish the reports referred to in Article 13 every six months.

Moreover, they must make publicly available at least once a year and within 30 days following the adoption of the audit implementing report:

a) a report outlining the outcome of the systemic risks assessment;
b) the risk mitigation measures that have been implemented;
c) the audit report;
d) the audit implementation report.

Article 33(2) DSA proposal envisages ample exceptions to the publication of the reports, as VLOPs are granted the possibility to remove information from the reports when they consider that such information may lead to the disclosure of confidential information of the platform or of the users, may cause vulnerabilities to the security of the service, undermine public security or harm users. If one of these conditions apply, the complete reports are transmitted only to the DSC of establishment and to the Commission.

2.5.7. Standards, codes of conduct and crisis protocols

The last section of Chapter III DSA includes four final provisions on due diligence obligations.

Pursuant to Article 34 DSA proposal, the Commission must support the development and update of voluntary standards by European and international standardization bodies. These voluntary industry standards are aimed at facilitating compliance with a number of due diligence obligations, such as the ones concerning the submission of notices under art. 14 and by trusted flaggers, transparency in advertising and auditing.

Article 35(1) requires the Board and the Commission to facilitate the definition of codes of conduct to support the application of the DSA regulation, particularly with regard to addressing illegal content and systemic risks. The Commission and the Board must ensure that the codes of conduct define specific commitments and key performance indicators (KPIs) and regularly evaluate the results achieved vis à vis the KPIs.[156]

Article 36 refers specifically to codes of conduct - to be negotiated between online platforms and other relevant stakeholders - to achieve transparency in online advertising beyond the minimum requirements set out by Articles 24 and 30.

[156] Article 35 DSA proposal, paragraphs 3 to 5.

Article 37 deals with the crisis protocols that may be drawn up only in times of extraordinary crises concerning public security or public health. The Commission may be recommended by the Board to promote the drawing up of crisis protocols in cooperation with VLOPs and, where needed, other online platforms. Possible measures include displaying information on the crisis as provided by Member States authorities and adapt the resources invested in compliance with Articles 14, 17, 19, 20 and 27 in light of the necessities posed by the extraordinary circumstances.