


RECOMMENDATIONS PAPER

December 2020

Sally Broughton Micova
Alexandre de Streel

DIGITAL SERVICES ACT

DEEPENING THE INTERNAL MARKET
AND CLARIFYING RESPONSIBILITIES
FOR DIGITAL SERVICES



The CERRE recommendations are based on a preparatory reflection paper and a workshop which took place in October 2020 with the following CERRE members: AGCOM, Facebook, Ofcom, Snap Inc., Vodafone. During the workshop, these participating members made very useful comments and suggestions, including a number of views which have not necessarily been accepted by the authors. A non-attributable summary of these, as well as the preparatory reflection paper, will be published separately on the CERRE website.

The recommendations presented in this paper were prepared by a team of academics including Sally Broughton-Micova and Alexandre de Streel. The academic team also benefited greatly from very useful comments by Martin Husovec. As provided for in CERRE's by-laws and the procedural rules from its "Transparency & Independence Policy", this report has been prepared in strict academic independence. At all times during the development process, the research authors and the CERRE Co-Academic Directors and Director General remain the sole decision-makers concerning all content in the report.

© Copyright 2020, Centre on Regulation in Europe (CERRE)
info@cerre.eu
www.cerre.eu



Table of contents

1. Introduction.....	4
2. Scope	6
3. Responsibility with limited liability	9
4. Harmonised notice and take-down.....	12
5. Enforcement.....	15

01

INTRODUCTION

1. Introduction

October 2020 brought further clarity on the shape of the **Digital Services Act (DSA)**, promised by the European Commission in its Digital Strategy Communication earlier in the year.¹ The European Parliament adopted three resolutions which have been prepared by the IMCO, the JURI and the LIBE Committees.² The Commission reported some of the findings from its consultations with the public and with stakeholders on deepening the internal market and clarifying responsibilities in respect of digital and on need to create ex ante regulatory instruments to better control the large online platforms that may act as gatekeepers services.³ These and their consultations with Member States have helped to crystallise the Commission's plans, which were presented by Commission Vice-President Margrethe Vestager in a speech on 29 October.⁴ The following points seem to have been established:

- The DSA will update the e-Commerce Directive (ECD) to place **more responsibility** on platforms and allow them to exercise their responsibilities more effectively to deal with **illegal** content.
- Fair competition issues and gatekeeping functions will be addressed in a **separate Digital Markets Act**.
- The **basic principles** of the ECD, including country of origin, limited liability, and the prohibition of monitoring and ex-ante removals were widely supported and **will be maintained**.
- There will likely be some form of **differentiation** in the treatment of services.

The separation of the competition and fairness issues into a separate act will allow the DSA to be tailored to the prevention harm from content and dangerous products. The fact that the most recent communications from the Commission refer only to **illegal** content seems to indicate a further narrowing of focus, leaving out content that is not illegal but may be harmful to all or some users.

Crucial open questions remain:

- Exactly what services will be in scope?
- How will responsibility be attributed with limited liability?
- What should harmonisation of notice and take-down look like?
- How will it be enforced?

This paper aims to contribute to the resolution of these open questions and inform the drafting of the DSA. It addresses each of these questions in turns and makes clear recommendations for each.

¹ Communication from the Commission of 19 February 2020, Shaping Europe's digital future, COM(2020) 67.

² https://www.europarl.europa.eu/doceo/document/TA-9-2020-10-20-TOC_EN.html

³ Some initial results have been shared by Commission officials, for example in slides shared as Working Paper WK 11834/2020 INIT on 27 October 2020. The consultations were held in summer 2020 and full responses can be found 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> and <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers>

⁴ Full text of the speech. https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/speech-executive-vice-president-margrethe-vestager-building-trust-technology_en

02

SCOPE

2. Scope

- The DSA should require online service providers to **designate a representative in the EU**, if not established within a member state, as done in the GDPR.
- The DSA should establish a **mechanism for determining jurisdiction** where there are claims by multiple member states.
- The DSA should reduce the list of conditions under which member states can derogate from the country of origin principle in line with the AVMSD.

There is clear appetite among policymakers in the Commission and the Parliament for the scope of the DSA to encompass services that are not established in the EU. There is precedent for three different options in recent EU legislation. The 2018 revision of the *Audiovisual Media Services Directive* (AVMSD), brought into scope video-sharing platforms that have a parent or subsidiary undertaking that is established in a member state or it is part of a group where an undertaking is established in a member state.⁵ This option would leave out services that have neither but still are used and accessed within the EU. The *Platform-to-Business Regulation* applies to online intermediation services and search engines, irrespective of their place of establishment, if their services are provided to business users that are established in the EU and that offer goods/services to consumers in the EU.⁶ The weakness of this option is the lack of a focal point for engagement in the processes of self and co-regulation that feature heavily in the governance of content. We recommend the option devised in the GDPR, which applies to companies that offer goods or services to individuals in the EU,⁷ and requires those not established in the EU to designate a representative in the EU.⁸ **The DSA should apply to services provided to individuals or businesses in the EU and those companies providing such services that are not established in the EU should be required to designate a representative.**

The ECD's country of origin principle is not complemented by provisions on establishing jurisdiction where there may be claims from multiple member states. Given the transnational nature of many of these companies, **the DSA should contain a mechanism like the one in the AVMSD for determining jurisdiction including the maintenance of a transparent centralised database by the Commission.**⁹

In addition, the ECD currently contains an extensive list of conditions under which member states can derogate from the country of origin principle. This list of **derogation conditions**, which are described in Article 3(4a) of the ECD, **should be reduced** and brought in line with what has been done in the AVMSD.¹⁰ Such reduction would stimulate the digital single market and the development of digital start-ups and scale-ups in Europe. Derogation should be limited to instances in which there is a serious risk to public security or public safety. Consumer protection should no longer be a basis

⁵ Directive 2010/13 of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), OJ [2010] L 95/1, as amended by Directive 2018/1808, Art. 28(a)


⁶ Regulation 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, OJ [2019] L 186/55, art.1(2).

⁷ Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation), OJ [2016] L 199/1, art.3 and European Data Protection Board Guidelines 3/2018 of 12 November 2019 on the territorial scope of the GDPR.

⁸ GDPR, art.27.

⁹ See AVMSD, art. 2(5, 5a, 5b & 5c)

¹⁰ AVMSD, art.3(2).



for derogation given the substantial strengthening of the EU consumer acquis since the enactment of the ECD.¹¹

The social media, video-sharing, messaging and other platforms that *host* content as understood in the ECD are part of wider ecosystems of services. A range of online services can be involved in enabling the dissemination of illegal content, such as online payment platforms, advertising intermediaries, auto-complete service, domain registers and others. The DSA should recognise that effectively combatting the dissemination of illegal content involves not only those platforms that are hosts or conduits for content. The DSA should, therefore, be part of a concerted and coordinated approach that may also include other areas of law and enforcement.

¹¹ Such as Directive 2005/29 of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, OJ [2005] L 149/22, as amended by Directive 2019/2161; Directive 2011/83 of the European Parliament and of the Council of 25 October 2011 on consumer rights, OJ [2011] L 304/64, as amended by Directive 2019/2161; Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ [2019] L 136/1.

03

RESPONSIBILITY WITH LIMITED LIABILITY

3. Responsibility with limited liability

- The DSA should clarify the conditions under which safe harbour can be lost so as to **avoid disincentivising services from taking preventive action** against illegal content.
- The DSA should harmonise rules aimed at achieving **procedural accountability** grounded in principles of **appropriateness and proportionality**. Therefore, digital platforms that, by their nature (user base, functionality, reach, role), pose a greater risk should be subject to more obligations than lower risk ones, and the DSA should not impede – and should, on the contrary, encourage – the development of start-ups and scale-ups in Europe.
- The DSA should provide an EU-wide legal basis for imposing **additional specific preventive measures** on services.

The liability regime in the ECD will be preserved, but it is not without shortcomings. In establishing responsibility for digital services, the DSA can remedy for some of these. One of the key areas for improvement is around the passivity criterion for hosting and there have been several calls to either abandon or to clarify it. The main concern behind the passivity criterion is that it potentially *discourages* voluntary preventive measures by the service providers, which may fear losing their safe harbour by implementing them. The ECD leaves it up to member states to determine the liability of services once they have lost safe harbour, so this disincentive may be stronger in some member states than others.


The DSA should give more clarity as to the conditions attached to the liability exemptions for services. The DSA should specify that *activity* aimed at preventing the dissemination of illegal content should not result in the loss of 'safe harbour'. Instead, online platforms should be expected to undertake preventive measures and be required to comply with rules aimed at achieving procedural accountability without prejudice to the underlying liability regime. The AVMSD's distinction between editorial responsibility and the responsibility derived from the organisation of content can be helpful here. The non-exhaustive list of measures expected to be taken by video-sharing platforms outlined in the AVMSD contains ones that are elements of notice and take down procedures¹² or functionalities afforded to users that allow them to take responsibility for exposure to legal content¹³. Digital services should be able to put in place measures for the identification and removal of illegal content and make their best efforts to prevent harm from the creation and dissemination of such content without automatically losing their exemption from liability.

Removing disincentives for taking preventive measures is not sufficient to ensure digital services effectively protect users from the harms associated with illegal content. Services **should be held responsible for making effective best efforts to protect users through harmonised rules establishing procedural accountability**. A procedural accountability approach means that regulators investigate and monitor, on the one hand, services' systems for compliance with the principles and objectives set out in law (without having to specify the measures those services might implement to meet those objectives) and, on the other hand, governance procedures, incentivizing services to adhere to principles of good governance.

There is currently significant information asymmetry between providers of digital services and regulators. Therefore the DSA should also **establish transparency and reporting obligations and mechanisms to enable access to information needed to assess how services are**

¹² Such as those in Art. 28(b)(3) lines d, e, and i that cover systems for flagging and reporting content and handling complaints.

¹³ such as those in Art. 28(b)(3) lines f, g and h that cover age verification, content rating and parental controls.



achieving the policy goals. It could set principles-based minimum standards for 'notice-and-takedown' procedures and proactive measures to facilitate platforms' detection and the cooperation with public enforcement authorities. Harmonized procedural accountability rules ensure oversight of the policies, processes and tools put in place by digital services, providing the benchmarks and information required for enforcement.

Though the issues of dominance and designation of services for special treatment due to their size seem to be now part of the planned Digital Markets Act, there remains an appetite for differentiated treatment of platforms, evident in the resolutions adopted by the European Parliament and in recent Commission communications. **Appropriateness and proportionality should be guiding principles of the DSA**, and procedural accountability marries well with this principle. All services would need to abide by the same set of procedural rules, but their obligations, for example reporting requirements, should be tailored their size, type and reach.¹⁴ If Europe wants to stimulate the development of start-ups and scale-ups, it is of the utmost importance that the DSA's rules should not become a barrier to entry or reason for the collapse of smaller services. At the same time, content-sharing services that have become so large and so important in the lives of citizens that they are now hosting part of the public space would face more extensive obligations, which could be detailed in codes of conducts or other instruments approved by regulatory authorities.

Size and reach should not be the only determinants. Obligations should also be appropriate to the type of harm in question, which may depend on the nature of the content, the business model of the service, design features or other characteristics. For example, the procedural rules for dealing with Child Sexual Abuse Material (CSAM) should be suitable to the egregious nature of the harm and the requirements of related criminal investigations, as, for the most part, they are already.¹⁵ The actual measure taken to combat CSAM might vary across services depending on the functions they offer users, so one that enables users to share content in closed groups might use machine detection and removal based on content id databases, among other measures, while a cryptocurrency service might take other measures aimed at identifying use by known offenders or patterns that would indicate the trade is such content.

Holding digital services accountable requires some consequences for not adhering to the procedural rules. In order to avoid sidestepping the existing ECD framework, the possibility would be to expect "best efforts" implementation as a baseline to avoid any liability. **The DSA should provide an EU-wide legal basis for imposing additional specific preventive measures** for use if services demonstrably fail to meet their obligations, which would be dealt with by the courts, under the coordination of the Court of Justice jurisprudence.

¹⁴ The size of a service should be measured not solely on the number of users, but also the extent to which it is used and other indications of market share and pervasiveness. In the context of the Digital Markets Act, indicators for large gatekeepers power will be defined. See the CERRE Recommendation papers for a list of criteria and indicators to designate Large Gatekeeper Platform.

¹⁵ See Directive 2011/93 of the European Parliament and of the Council of 13 December 2011 on combatting the sexual abuse and sexual exploitation of children and child pornography OJ [2011] L 335/1, art.25. and Report from the Commission of 16 December 2016 assessing the implementation of the measures referred to in Article 25 of Directive 2011/93 on combatting the sexual abuse and sexual exploitation of children and child pornography, COM(2016) 872.

04

HARMONISED NOTICE AND TAKE-DOWN

4. Harmonised notice and take-down

- The DSA should set out **standards for notice and take down** that are designed to cover **automatic** and human means.
- The DSA should include rules aimed at **protecting users** from harms related to illegal content and at protecting their **fundamental rights** as individuals and collectives.
- The DSA should institute requirements for **alternative dispute resolution** to be made available in each member state and in all necessary languages.

When the ECD was drafted, it was not assumed that notice and takedown of illegal content would be largely conducted by automated means and by the services themselves. This is now largely the case. Even smaller services use third party tools and collaborate with larger services for the automated detection and removal of CSAM and terrorist content. Illegal hate speech including racism and xenophobia arguably require more nuanced understandings and balancing of fundamental rights, but the largest platforms are also using in-house automated tools to identify and take down such content as well. For example, in the third quarter of 2020, 93.88% of all video removals on YouTube were based on automatic detection, and, of the 22.1 million items of hate speech content actioned by Facebook, only 5.5% was flagged by users.¹⁶ When it comes to illegal content this type of preventive action should be encouraged by procedural rules on notice and take down, but with adequate safeguards for freedom of expression.

The DSA should set out principles-based standards for notice and take down that are designed to cover automatic and human means and that include adequate safeguards for fundamental rights. There are existing standards for notice and take down in specific areas. The DSA's standards could be based on the measures recommended by the European Commission in its Recommendation on measures to effectively tackle illegal online content as well as on the measures foreseen for video-sharing platforms by the AVMSD.¹⁷ They could also be based on principles and measures to which many major service providers committed through multi-stakeholder initiatives, such as the Santa Clara Principles on Transparency and Accountability in Content Moderation, the Voluntary Principles to Counter Child Sexual Exploitation and Abuse and the EU Code of Conduct on Countering Illegal Hate Speech Online.¹⁸ The following is an non-exhaustive list of actions for which procedural rules should be considered and applied to platforms when appropriate according to the business model and the activity of the platform and in line with the principle of proportionality. Indeed, it is key that the application of those principles do not impede the development of start-ups and scale-ups in Europe.

¹⁶ See YouTube's transparency report https://transparencyreport.google.com/youtube-policy/removals?hl=en_GB and Facebook's transparency report on this issue <https://transparency.facebook.com/community-standards-enforcement#hate-speech>

¹⁷ Commission Recommendation 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, OJ [2018] L63/50, Points 5-28; AVMSD, Article 28b. In addition, the proposed reforms would also meet the Santa Clara Principles on Transparency and Accountability in Content Moderation:.

¹⁸ The Santa Clara Principles: <https://www.santaclaraprinciples.org/>; The voluntary principles <https://www.gov.uk/government/publications/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse#the-voluntary-principles>; The Code of Conduct on Hate Speech: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

For effective **protection from harms** stemming from illegal content

- Provide transparent and user-friendly mechanisms for users to report or flag illegal content or behaviour related to its dissemination;
- Establish networks of or otherwise engage with “trusted flaggers” in a transparent manner;
- Remove content identified as illegal by automated means or human flagging;
- Prevent search results from returning illegal content;
- Prevent the monetisation of illegal content;
- Expeditious removal of content aimed at immediate incitement to violence;
- Targeted monitoring to ensure that identical instances of the same material are not re-uploaded by any user or that similar instances are not uploaded by the same user;
- Establish mechanisms for reporting illegal activity to relevant authorities;
- Preserve evidence of crimes in a safe manner when required by relevant authorities or investigators and in full compliance with EU privacy rules.¹⁹

For effective protection of fundamental rights:

- Accompany content or account removals with specific explanatory notices and inform flaggers of the outcome of their flagging;
- Report regularly on numbers of content and account removals, with additional descriptive details appropriate to the nature of the service and by the type of the platform;
- Provide transparent, easy-to-use and effective procedures for the handling and resolution of user appeals and complaints;
- Provide mechanisms for handling “super complaints” or collective complaints about systemic issues, such as discriminatory tendencies in content moderation;
- Support and participate in independent alternative dispute resolution in all the necessary languages.

Most measures currently being used by major digital services are for removing and acting on individual content and providing options to appeal specific removal decisions. In order to adequately protect fundamental rights, services need to be able to address tendencies and handle complaints about how systems are working for groups of users. Providing adequate data on removals, and notice of the reasons for removals to users, combined with accessible and easy complaints mechanisms for individuals and groups to use is crucial. Users also need external means through which they can challenge decisions by services that may affect fundamental rights. **Access to dispute resolution should be made as simple as possible**, which is why Alternative Dispute Resolution (ADR) systems should be available in the country and language of where the alleged victim is located. These ADR systems should be **independent and well-funded** and provide for rapid, effective and impartial relief.

¹⁹ These might include civil society and human rights organisations investigating incidents of war crimes or abuses and not solely national law enforcement.

05

ENFORCEMENT

5. Enforcement

- DSA should encourage **codes of conduct** and set criteria for how they are established and their implementation monitored.
- The DSA should include obligations aimed at **ensuring regulatory authorities have sufficient access to information** with which to assess services' procedures and compliance.
- The DSA should establish the means for **co-ordination among member states' regulatory authorities** relying as much as possible on existing mechanisms.

For the enforcement of the DSA, **codes of conduct should continue to be encouraged** as they can be very useful in dynamic industries where the best ways to achieve regulatory goals may not be static and will require ongoing dialogue with industry. The **DSA should impose criteria on how such Codes are established and their implementation monitored** in order to increase their legitimacy, their effectiveness and their compliance with fundamental rights. The DSA could follow the same approach already taken in the AVMSD, which states that codes should be accepted by the main actors representing different interests at stake, have clear objectives, and that their implementation should involve regular independent and transparent monitoring, and effective and proportionate sanctions.²⁰ Such codes can set specific targets for measures, establish cooperation protocols, detail reporting requirements, as well as include commitments to making technology available to others and other forms of collaboration.²¹

There is also a **need for the DSA to establish rules to ensure transparency and access to information for regulatory authorities**. This is of the utmost importance given the large information asymmetry between the digital platforms and the regulatory authorities. This kind of information is essential for the assessment of such procedures by regulators. National regulators will need to be able to monitor the notice and take down measures, the level of transparency in the process used by services, any evidence of due diligence in coordination with law enforcement, etc.²²


National regulatory authorities have already been tasked by the AVMSD with assessing the measures undertaken by video-sharing platforms to protect users and combat illegal content. In establishing rules for procedural accountability and setting out their enforcement, **the DSA should not create duplicate requirements for services also within the scope of other EU laws**, in particular the AVMSD. For example transparency or reporting measures implemented to enable the monitoring by national regulators required by the AVMSD should, wherever possible, also serve for the enforcement of the DSA.

Given the nature of digital services, coordination, cooperation and mutual assistance among national regulators will be crucial to enforcement. There has already been great progress in this through the

²⁰ See AVMSD, new Article 4a introduced by Directive 2018/1808.

²¹ For example, governments and providers of online services made a number of commitments as supporters of the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online, including ones pertaining to the quality and enforcement of community standards and immediate action upon detection, regular reporting and designing of algorithms so as not to amplify terrorist and violent extremist content. The Global Internet Forum for Counter Terrorism (GIFCT), which was a joint investment in technology and identification databases by tech companies, coordinates a Content Incident Protocol, which has already been used to coordinate rapid detection and removal during ongoing incidents, but many online service providers are not yet participating.

²² If in the process of the negotiations the scope of the DSA does end up covering also harmful but legal content, then transparency will be also highly important to end users as well as regulators, for example so that they can understand why they are being served certain types of content or why their content is frequently flagged.



European Regulators Group for Audiovisual (ERGA), the creation and then the reinforcement of the Consumer Protection Cooperation (CPC) Network²³ and the increasing use of the Internal Market Information (IMI) System.²⁴ **The DSA should set out a formal mechanism, for instance with the establishment of an EU Board among the national supervisory authorities, for cooperation among national regulators** that draws upon these and other existing means. Cooperation between member state regulators and ones from non-EU states should also be encouraged due to the transnational nature of the services and the harms. In case of serious failures by large services, especially involving users from multiple member states, it may be necessary to have an EU level body assessing and responding.

²³ Regulation 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation 2006/2004, OJ [2017] L 345/1.

²⁴ Regulation 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC (the IMI Regulation), OJ [2012] L 316/1, as amended by Directives 2013/55, 2014/60, 2014/67 and Regulation 2016/1191, 2016/1628 and 2018/1724.



cerre

Centre on Regulation in Europe

📍 Avenue Louise, 475 (box 10)
1050 Brussels, Belgium

📞 +32 2 230 83 60

✉️ info@cerre.eu

🌐 cerre.eu

🐦 [@CERRE_ThinkTank](https://twitter.com/CERRE_ThinkTank)