



cerre

Centre on Regulation in Europe


REPORT

December 2020

Sally Broughton Micova
Alexandre de Stree

DIGITAL SERVICES ACT

**DEEPENING THE INTERNAL MARKET
AND CLARIFYING RESPONSIBILITIES
FOR DIGITAL SERVICES**



The project, within the framework of which this report has been prepared, has received the support and/or input of the following organisations: 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 accepted by the authors.

The Issue Paper and the recommendations 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. The non-attributable summary of the discussion was prepared by Claire-Marie Healy, project manager at CERRE.

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

TABLE OF CONTENTS	2
ABOUT THE AUTHORS	3
BACKGROUND AND CONTEXT	5
ISSUE PAPER	7
1 Introduction	7
2 The e-commerce Directive and its reform	8
2.1 Pillars and goals of the Directive.....	8
2.2 Need for reform	10
3 Deepening the internal market	11
3.1 Strengthening the internal market clause	11
3.2 Application to non-EU providers	12
4 Clarifying the responsibilities for a safer Internet	13
4.1 Evolution of the rules	13
4.2 Critique and shortcomings of the liability regime	18
4.3 Reforming the baseline regime: strengthening procedural accountability	20
4.3.1 Increased role for users and trusted flaggers	20
4.3.2 Preventive measures	21
4.4 Aligning responsibility with risks	22
5 Improving oversight and enforcement	22
5.1 Existing rules	22
5.2 Avenues for reforms	24
5.2.1 Enforcement with public authorities	24
5.2.2 Enforcement with private bodies.....	25
6 References	26
WORKSHOP DISCUSSION SUMMARY	30
RECOMMENDATIONS PAPER	35
1 Introduction	35
2 Scope	36
3 Responsibility with limited liability	37
4 Harmonised notice and take-down	39
5 Enforcement	41
ABOUT CERRE	43

ABOUT THE AUTHORS



Sally Broughton Micova is a CERRE Research Fellow and a Lecturer in Communications Policy and Politics at the University of East Anglia (UEA). She is also a member of UEA's Centre for Competition Policy. Her research focuses on media and communications policy in Europe. She completed her PhD in the Department of Media and Communications at the London School of Economics and Political Science (LSE), after which she was an LSE Teaching and Research Fellow in Media Governance and Policy and Deputy Director of the LSE Media Policy Project.



Alexandre de Steel is an Academic Co-Director at CERRE and Professor of European Law at the Universities of Namur and Louvain in Belgium. He is also the Director of the Research Centre for Information, Law and Society (CRIDS), focusing his research on Regulation and Competition Law in the network industries. Alexandre regularly advises international organisations and national regulatory authorities on regulatory and competition issues in network industries. He holds a PhD in Law from the European University Institute.



BACKGROUND AND CONTEXT

BACKGROUND AND CONTEXT

This research report comprises of several documents, including an **Issue Paper** prepared by a team of academics, a **non-attributable summary of the discussion** organised in October 2020 with support from representatives of the CERRE members and the CERRE academic team, and the **recommendations paper** drafted by a team of academics on the basis of the Issue Paper and the related discussion.

This report is in line with CERRE's ambitions to remain at the cutting edge of regulatory developments in the digital and network industries and to constructively and independently contribute to the EU policy making process.

Objective and topics

Building on previous and ongoing CERRE work¹ on the regulation of the online platform economy, this report considers the question of responsibility of online platforms and content moderation and how this can be addressed in the DSA. The project will also consider how an effective system for regulatory oversight could be designed. How coordination between Member States should be improved? How should the relationship between online platforms and oversight bodies be optimised?

Methodology

The responses to the above questions were developed and finalised with the following steps:

- The CERRE academic team prepared an **Issue Paper** that summarised on the basis of the most recent academic literature and policy reports, the issues and their trade-offs as well as the main policy proposals made so far.
- The Issue Paper underpinned a **brainstorming discussion during an exclusive e-workshop** reserved to representatives of the CERRE members supporting the project and the academic team. A **summary** of the discussion, underlining the main issues, trade-offs and possible solutions as well as divergent views, was also written after the webinar, respecting its Chatham House Rule.
- On the basis of the Issue Paper and the related brainstorming discussions, the CERRE academic team drafted a **recommendations paper** aimed at feeding the policy makers' reflections for the DSA.

¹ See CERRE Report on liability for online hosting platforms, <http://www.cerre.eu/publications/liability-online-hosting-platforms-should-exceptionalism-end>, the CERRE report on artificial intelligence tools and online hate speech, September 2018; <https://www.cerre.eu/publications/artificial-intelligence-tools-and-online-hate-speech>, February 2019; and the CERRE recommendations on the DMA, November 2020. <https://cerre.eu/publications/digital-markets-act-economic-regulation-platforms-digital-age/>



ISSUE PAPER

ISSUE PAPER

1 Introduction

In its 2020 Digital Strategy Communication of February,² the Commission announced that the proposal of the **Digital Services Act package** would include one pillar aiming at deepening the internal market and clarifying the responsibilities of digital services. This pillar will possibly amend or complement the e-commerce Directive.³

In their Inception Impact Assessment of June 2020, the Commission services indicate that they are considering the following **three policy options**:⁴

1. A limited **legal instrument would regulate online platforms' procedural obligations**, essentially making the horizontal provisions of the 2018 Recommendation on illegal content online binding.⁵ This would build on the scope of the e-Commerce Directive, focusing on *services established in the EU*. It would lay out the *responsibilities* of online platforms with regard to sales of illegal products and services, dissemination of illegal content and other illegal activities of their users. They would include proportionate obligations such as effective notice-and-action mechanisms to report illegal content or goods, as well as effective redress obligations such as counter-notice procedures and transparency obligations. This option would neither clarify nor update the liability rules of the e-Commerce Directive for platforms or other online intermediaries.

2. **A more comprehensive legal intervention**, updating and modernising the rules of the e-Commerce Directive, while preserving its main principles. It would clarify and *upgrade the liability and safety rules* for digital services and remove disincentives for their voluntary actions to address illegal content, goods or services they intermediate, concerning online platform services in particular. Definitions of what illegal is online would be based on other legal acts at EU and national level.

It would harmonise a set of *specific, binding and proportionate obligations, specifying the different responsibilities*, especially for online platform services. In addition to a basic set of generally applicable obligations, further asymmetric obligations may be needed depending on the type, size, and/or risk a digital service presents, as well as a cooperation framework and due process requirements for crisis situations. Obligations could include:

- (i) harmonised obligations to maintain '*notice-and-action*' systems covering all types of illegal goods, content, and services, along with 'know your customer' schemes for commercial users of marketplaces,
- (ii) rules ensuring effective *cooperation of digital service providers with the relevant authorities and 'trusted flaggers'* (e.g. the INHOPE hotlines for a swifter removal of child sexual abuse material)⁶ and reporting as appropriate,
- (iii) *risk assessments* could be required from online platforms for issues related to exploitation of their services to disseminate some categories of harmful – but not illegal – content, such as disinformation,
- (iv) more effective *redress and protection* against unjustified removal for legitimate content and goods online, or
- (v) a set of transparency and *reporting obligations* related to these processes.

² Communication from the Commission of 19 February 2020, Shaping Europe's digital future, COM(2020) 67.

³ Directive 2000/31 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 (Directive on electronic commerce), OJ [2000] L 178/1. Many other EU rules are also applicable to online platforms and are described in de Streel, Kuczerawy and Ledger (2019).

⁴ <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>

⁵ Commission Recommendation 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, OJ [2018] L63/50.

⁶ <https://www.inhope.org/EN>

Beyond personal data protection rights and obligations, it would also explore transparency, reporting and independent audit obligations to ensure accountability of *algorithmic systems for (automated) content moderation* and recommender systems, as well as online advertising and commercial communications, including political advertising and micro-targeting aspects. Such measures would enable effective oversight of online platforms and would support the efforts to tackle online disinformation. Issues related to legal clarity around smart contracts would also be considered.

It would explore extending coverage of such measures to all services directed towards the European single market, including services *established outside the Union*, with a view to identifying the most effective means of enforcement.

The instrument would also establish *dissuasive and proportionate sanctions* for systematic failure to comply with the harmonised responsibilities or the respect of fundamental rights.

3. Options for creating an effective system of regulatory oversight, enforcement and cooperation across Member States, supported at EU level. These options, in complement to the previous options, would aim to reinforce the updated set of rules (as per Option 1 or 2 above). They should provide for *effective EU-wide governance* of digital services through a sufficient level of harmonisation of rules and procedures. Based on the country of origin principle, these options would allow Member States' authorities to deal with illegal content, goods or services online, including swift and effective cooperation procedures for cross-border issues in the regulation and oversight over digital services. Public authorities' capabilities for supervising digital services would also be strengthened. They would be provided with appropriate powers, potentially supported at EU level, to effectively and dissuasively sanction systemic failure of services established in their jurisdiction to comply with the relevant obligations. Options for effective judicial redress would be explored too.

This Issue Paper is organised as follows. After this introduction, Section 2 deals with the e-commerce Directive and the need for its reform. Section 3 deals with deepening the Digital Single Market. Section 4 deals with clarifying (aka strengthening) responsibilities of online platforms for a safer Internet. Section 5 deals with improving oversight of the platforms and enforcement of the rules. Finally, Section 6 lists the questions for the discussion at the webinar.

This issue paper is based on previous work done by CERRE on platforms liability⁷ as well as studies co-authored by CERRE academics for the European institutions.⁸

2 The e-commerce Directive and its reform

2.1 Pillars and goals of the Directive

In 2000, when online platforms were in their infancy, the e-commerce Directive (ECD) established a regulatory regime based on **four pillars**. The first pillar sets the **country of origin principle** to strengthen the internal market.⁹ It implies an online platform is only subject to the rules of the EU member state where it is established and may then provide its services across the 26 other Member States without being subject to the rules of those other States. Unless there are exceptional circumstances related to public policy, health, security or protection of consumers and investors, Member States may not restrict the freedom to provide information society services from another Member State.¹⁰

The second pillar of the EU regime creates an **exemption from the national liability regime** to which the hosting platform is subject to, and harmonises the conditions at the EU level for such

⁷ In particular <https://cerre.eu/publications/liability-online-hosting-platforms-should-exceptionalism-end/> and <https://cerre.eu/publications/playing-field-audiovisual-advertising/>

⁸ In particular de Streel and Husovec (2020) and de Streel et al. (2020).

⁹ ECD, art 3.

¹⁰ This safeguard clause has been very rarely used by the Member States: Commission Staff Working Document of 11 January 2012, Online services, including e-commerce, in the Single Market, SEC(2011) 1641, p.21.

exemption.¹¹ A hosting platform can escape liability for illegal material uploaded by users when it does not have knowledge of the illegality or, upon obtaining such knowledge, it acts expeditiously to remove or disable the access to the material (notice-and-takedown). The Court of Justice of the European Union has interpreted these conditions by distinguishing between two different types of services. On the one hand, services of a mere technical, automatic and passive nature – where the platform plays a neutral role – can benefit from the liability exemption. On the other hand, services of a more active nature – such as optimising the ranking of offers for an ecommerce platform – cannot benefit from the exemption.¹²

The third pillar of the EU regime consists in the **prohibition for EU Member States to impose a general obligation** on the hosting platforms to monitor the hosted material.¹³ The Court of Justice of the EU has drawn a line between general monitoring measures, which are prohibited,¹⁴ and specific monitoring measures, particularly in case of suspected violation of intellectual property rights, which are allowed when having achieved a fair balance between the fundamental rights of the different stakeholders.¹⁵

The fourth pillar of the EU regime is the **encouragement of co- and self-regulation** to implement the rules and principles of the Directive.¹⁶ Notably, the Directive mentions the importance of involving consumers in the drafting of these Codes of conduct to ensure that the rules remain balanced. It also mentions the necessity of monitoring (in cooperation with Member States and the Commission), and the implementation of the Codes to ensure the effectiveness of the rules. As illustrated below, this provision has led to increasing reliance on co- and self-regulation to tackle certain types of illegal materials which are particularly harmful, such as child abuse content, terrorism content, hate speech or counterfeit goods.

As explained by the European Commission¹⁷, this legal regime pursues **four main objectives**.

¹¹ Directive 2000/31 on electronic commerce, art 14. In addition, two other categories of online intermediaries (mere conduits and caching) are also exempt from liability, but no subject to a notice and take down regime: Directive 2000/31 on electronic commerce, arts.12-13.

¹² Cases C-236/08 to C-238/08 *Google France v Louis Vuitton* EU:C:2010:159, paras 113 where the Court of Justice decided that: 'the exemptions from liability established in the directive cover only cases in which the activity of the information society service provider is 'of a mere technical, automatic and passive nature', which implies that that service provider 'has neither knowledge of nor control over the information which is transmitted or stored'; Case C-324/09 *L'Oreal et al. v. eBay* EU:C:2011:474, para.116 where the Court of Justice decided that: 'Where, the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability'; Case C-484/14 *Mc Fadden* EU:C:2016:689, para 62. Those cases are well explained in *Van Eecke* (2011), *Husovec* (2017), *Nordemann* (2018), *van Hoboken et al.* (2018).

¹³ ECD, art 15.

¹⁴ Case C-360/10 *SABAM v. Netlog* EU:C:2012:85 where the Court of Justice decided that the e-commerce Directive precludes: 'a national court from issuing an injunction against a hosting service provider which requires it to install a system for filtering information which is stored on its servers by its service users; which applies indiscriminately to all of those users, as a preventative measure, exclusively at its expense, and for an unlimited period; which is capable of identifying electronic files containing musical, cinematographic or audiovisual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright'. Also Case C-70/10 *Scarlet Extended v. SABAM* EU:C:2011:771.

¹⁵ Case C-314/12 *UPC Telekabel Wien v Constantin Film Verleih* EU:C:2014:192 where the Court of Justice decided that the injunction must: 'strike a balance, primarily, between (i) copyrights and related rights, which are intellectual property and are therefore protected under Article 17(2) of the Charter, (ii) the freedom to conduct a business, which economic agents such as internet service providers enjoy under Article 16 of the Charter, and (iii) the freedom of information of internet users, whose protection is ensured by Article 11 of the Charter' (at para.47 of the Case) and that such balance is found when the injunctions do not: 'unnecessarily deprive internet users of the possibility of lawfully accessing the information available and that they have the effect of preventing unauthorised access to protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right' (at para.63 of the case). Also more recently, Case C-484/14 *Mc Fadden*, para 96.

¹⁶ ECD, art 16.

¹⁷ Explanatory Memorandum of the Commission proposal for a directive on certain legal aspects of electronic commerce in the internal market, COM (1998) 586.

- The first was to **share responsibility for a safe Internet** among all the private actors involved together with good cooperation with public authorities. Thus, the injured parties should notify the hosting platforms of any illegality they observe and the hosting platforms should remove or block access to any illegal material of which they are aware. This should ensure timely private enforcement that may effectively complement public adjudication.
- The second objective was to **encourage the development of e-commerce in Europe** by increasing legal certainty on the role of each actor and by ensuring that the hosting platforms do not have an obligation to monitor the legality of all material they store. This would have been extremely costly, especially at a time when effective machine-learning-based technologies were in their infancy.
- The third objective was to strike a **fair balance between different fundamental rights** of the several stakeholders (such as the platforms, the users or the potentially injured parties), in particular privacy and the freedom of expression and information of the users, the freedom to conduct business of the platforms and the right to property including intellectual property of injured parties.¹⁸
- The fourth objective was to **strengthen the Digital Single Market** by adopting a common EU standard for a liability exemption, especially at a time when national rules and case law were increasingly divergent.

2.2 Need for reform

Since the adoption of the ECD, technology and markets have changed substantially. Online platforms are offering new types of services with the development of user-generated content and the progress of the collaborative economy blurring the lines between producers and consumers. Now users, but also platforms, play a more active role. Therefore, the criteria set by the ECD and the Court of Justice to divide the neutral and passive platforms taking advantage of the liability exemption from the active platforms that do not benefit from the exemption, are more difficult to apply and require clarification. Moreover, some online platforms have become very large. This is often attributed to cross-groups and within-groups network effects explained in the other stream of CERRE reflection on the DSA.¹⁹ As a result, the harm caused by illegal material is more massive as they affect many more users. At the same time, the financial, technological and human capacities of the platforms to prevent and remove such illegal material have also expanded. Large tech companies have developed effective machine-learning-based tools that identify and remove illegal or harmful content mostly before it is observed. These tools are widely used to combat child sexual exploitation and terrorist use of content platforms and, on some platforms, to detect hate speech and disinformation. For the protection of copyright, such tools have been found to decrease the costs for victims and to prevent harm caused by illegal material hosted by online platforms.²⁰ These evolutions triggered a call to reform the ECD rules and to increase the responsibility of the online platforms.²¹

Such reform should aim to protect citizens from illegal or harmful content and behaviour online while guaranteeing an appropriate balance among fundamental rights. This could be achieved by efficiently sharing and targeting the responsibility of detecting and removing illegal online content among the many actors involved in the diffusion of such material and evolving towards a system of 'cooperative

¹⁸ As protected by the Charter of Fundamental Rights of the European Union, art 7, 8, 11, 16 and 17.

¹⁹ Also Martens (2016).

²⁰ For an overview of the machine-learning-based techniques to detect copyrighted material, see Commission Staff Working Document, Impact Assessment on the modernisation of EU Copyright Rules, SWD (2016) 301, Annex 12.

²¹ Communication from the Commission of 25 May 2016, Online Platforms and the Digital Single Market: Opportunities and Challenges for Europe, COM(2016) 288.

responsibility²². As suggested in de Streel et al. (2020, p. 86-87), the regulatory framework could be based on the following principles:

- Provide sufficient and effective safeguards for **EU standards relating to all fundamental rights**, in particular, freedom of expression, the right to privacy, the prohibition of discrimination and the right to a fair trial/effective remedy;
- Strengthen the Internal Market and alleviate national regulatory fragmentation; this requires trust among the Member States;
- Ensure **a level playing field** between online and offline activities and ensure that what is illegal offline is also illegal online; the rules should also be **technological and business neutral** and not favour one technology or business model over others;
- Provide to all stakeholders involved in the removal of illegal and harmful online content the **right incentives to minimise the risk of errors**, of type I errors (over-removal) and of type II errors (under-removal);
- **Be appropriate and proportionate**, which could lead to a differentiation of rules according to the type of content (and its potential negative impact on the society) and according to the nature of the business model and the size of platforms (and their means and societal reach); and at the same time, the multi-layered regulatory framework to which differentiation leads should remain **coherent**;
- Be **sufficiently general** to be easily adaptable to technology and business models, which evolve quickly and often in unpredictable ways; to ensure legal certainty, these general rules could then be clarified by the European Commission in delegated or implementing acts or interpretative guidance;
- Be **enforced effectively**, on the basis of a smart combination of traditional State enforcement mechanisms with administrative and judicial authorities and alternative private enforcement mechanisms such as self- and co-regulation and out-of-courts dispute resolution tools.

3 Deepening the internal market

3.1 Strengthening the internal market clause

The **internal market clause is one of the greatest successes of the E-commerce Directive** as it is the cornerstone of the Digital Single Market. However, in order to be effective, this internal market clause needs to be accompanied by the confidence of the Member States (and their citizens) that the regulation in the country of establishment is sufficiently protective and effectively enforced. Such confidence requires, on the one hand, a harmonisation of the main rules aimed to protect users and, on the other hand, cooperation and mutual assistance between the competent authorities of the Member States in charge of enforcing the rules.

Fortunately, both have increased since the adoption of the ECD. First, the harmonisation of protection rules has substantially increased by reinforcing B2C consumer acquis (both at the substantive and institutional levels)²³ and AVMS rules²⁴, and the recent adoption of B2B protection rules (thanks to the new P2B Regulation)²⁵. Second, the tools for Member States cooperation have

²² As suggested by Helberger, Pierson and Poell (2018).

²³ Mainly: 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 and 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.

²⁴ 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

²⁵ 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.

also been strengthened with the establishment of the e-commerce expert group, the European Regulators Group for Audiovisual (ERGA), the creation and then the reinforcement of the Consumer Protection Cooperation (CPC) Network²⁶ and the increasing use of the Internal Market Information (IMI) System.²⁷

However, improvements are still possible, especially when it comes to the conditions under which the derogation can be used by the destination Member State to regulate an information society service provider established in another Member State. The substantive conditions, which are described in Article 3(4a) of the ECD, could be made more limited as it is now done in the AVMSD.²⁸ In particular, the derogation could be limited to public security, public health or public security. In addition, they could no longer be based on consumer protection given the substantial strengthening of the EU consumer acquis since the enactment of the ECD. The procedural conditions, which are described in Article 3(4b) of the ECD, could set some time limits and improve openness and transparency as it is done by the Transparency Directive.²⁹

Another possible area for improvement entails **further clarification of the notion of 'coordinated field'**, which frames the areas covered by the country of origin principle. Despite being thoroughly defined, the notion covers potentially very wide areas which are not altogether harmonised in the Directive. It includes requirements that the service provider needs to comply with as part of an information society service, such as requirements concerning qualifications, authorisation or notification; the pursuit of the activity of an information society service; the behaviour of the service provider; the quality or content of the service including those applicable to advertising; contracts and the liability of the service provider.

The eight exceptions to the internal market clause, contained in the Annex of the ECD, could also be reviewed to assess whether they are still justified in light of the EU harmonisation of national legislation that has taken place since the adoption of the Directive. This is particularly true for consumer protection rules, which means that the exception relating to contractual obligations for consumer contracts may no longer be justified.

3.2 Application to non-EU providers

The ECD applies to providers that are established in a Member State by referring to a **standard definition of establishment**: a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not constitute an establishment of the provider by themselves.³⁰ In recent years, there has been tension at Member State and EU level linked to the fact that some non-EU tech companies are providing services to EU citizens without necessarily abiding by EU (and national) rules.

Some of the more recently adopted EU legal instruments take other criteria into consideration to trigger the application of EU rules. This signals that the traditional criteria of the establishment may be no longer adequate.

²⁶ 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.

²⁷ 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.

²⁸ AVMSD, art.3(2).

²⁹ Directive 2015/1535, arts. 5 and 6. Interestingly, in Case C-390/18 *Airbnb Ireland*, ECLI:EU:C:2019:1112, the Court of Justice already draws a parallel between the derogation procedure of the ECD and the procedures of the Transparency and decides to impose the same sanction (unenforceability against individuals) when a Member State fails the procedural conditions, in particular a failure to notify to the Commission the national derogatory measures.

³⁰ ECD, recital 19.

- The *GDPR* applies to companies not established in the EU that offer goods or services to individuals in the EU or that monitor their behaviour.³¹ Companies not established in the EU but subject to the GDPR have to designate a representative in the EU, unless they process personal data occasionally and without a risk for individuals.³²
- The *AVMSD* provides that non-EU Video-Sharing Platforms are deemed to be established in a Member State if it has a parent or subsidiary undertaking that is established in that Member State or it is part of a group where an undertaking is established in that member state. It then goes on to settle how to determine which Member State has jurisdiction in case multiple Member States could claim jurisdiction.³³
- 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.³⁴

The ECD and its internal market clause could also cover the **online platforms that are not established in the EU** but provide their services to EU customers. To do so, the ECD could follow the systems adopted in more recent EU legislations such as imposing the designation of a representative in the EU (as set out in the GDPR).

The ECD could also cover how Member States should **handle multiple claims to jurisdiction within the EU** (as done with the AVMSD) and envisage including a transparent register listing the Member States having jurisdiction over a given information society service provider, which could be maintained by the European Commission.

4 Clarifying the responsibilities for a safer Internet

4.1 Evolution of the rules

Since the adoption of the ECD, the Commission first has clarified the general liability regime of the ECD by adopting a Communication in 2017, followed by a Recommendation in 2018.³⁵ These two instruments aim to improve the effectiveness and transparency of the notice-and-takedown process between the users and the platforms, stimulate preventive measures by online platforms and increase cooperation between providers of hosting services and the specific stakeholders (such as users, trusted flaggers and public authorities). Yet, although Member States should take into the utmost account the Recommendation, this legal act is not legally binding.³⁶

This Recommendation sets out the general principles for all types of illegal content, complemented by stricter principles for terrorist content because this material is particularly harmful.

- Regarding the **notice-and-takedown**, the Recommendation calls for procedures that (i) are effective, sufficiently precise and adequately substantiated, (ii) respect the rights of content providers with possibilities of counter-notices and out-of-court dispute settlement and (iii) are transparent.³⁷

³¹ 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.

³² GDPR, art.27.

³³ AVMSD, art.28(a).

³⁴ P2B Regulation, art.1(2).

³⁵ Communication of the Commission of 28 September 2017, Tackling Illegal Content Online. Towards an enhanced responsibility for online platforms, COM (2017) 555 and Commission Recommendation 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, OJ [2018] L63/50.

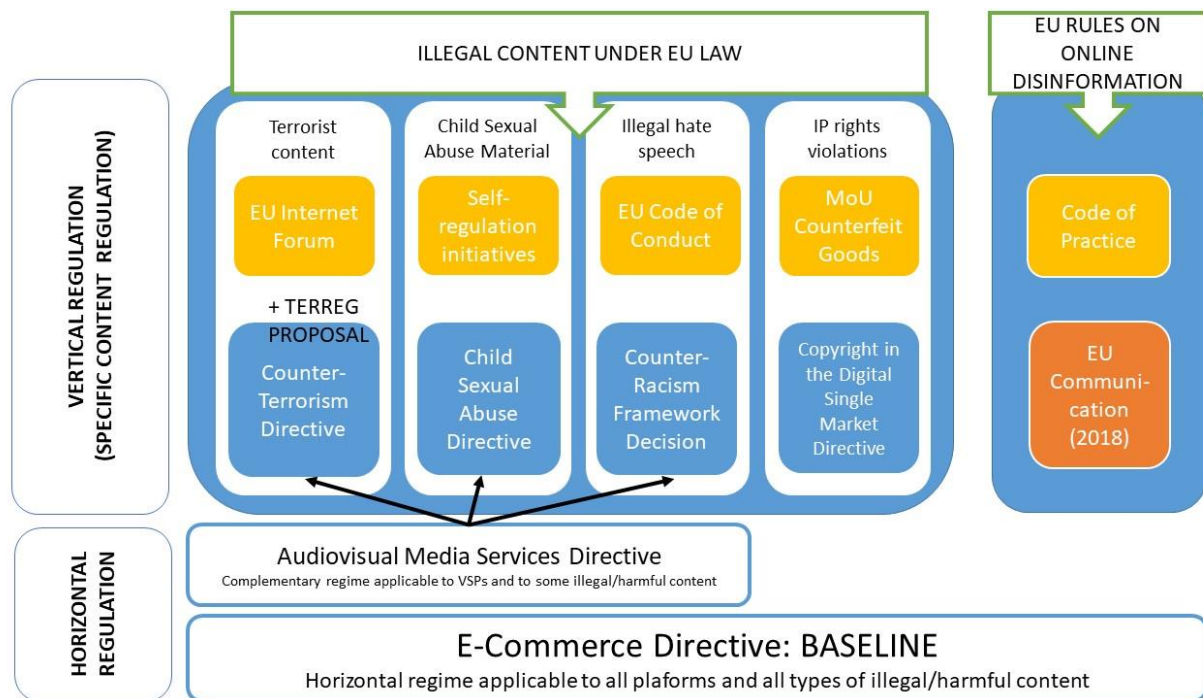
³⁶ TFEU, art.288. Case C-16/16P *Belgium v. Commission* EU:C:2018:79.

³⁷ Points 5-17 of the Recommendation 2018/334.

- Regarding **proactive measures**, the Recommendation encourages appropriate, proportionate and specific measures which could involve the use of automated means, provided some safeguards be in place, in particular human oversight and verification.³⁸
- Regarding **cooperation**, the Recommendation encourages close cooperation between the hosting services providers and the judicial and administrative authorities of the Member States, trusted flaggers (having the necessary expertise and determined on a clear and objective basis) and other hosting providers, especially smaller ones that may have less capacity to tackle illegal content.³⁹

Second, the baseline regime of the ECD has been complemented for particularly harmful illegal material by sectoral rules and co/self-regulatory measures, having increased the actions against those types of content as illustrated in Figure 1 below. The baseline regime is contained in the ECD, which applies to all categories of hosting platforms and all types of illegal content online. The Audiovisual Media Services Directive provides for additional rules applicable to Video-Sharing Platforms aimed at protecting the public, especially minors from a certain type of illegal and harmful content. In addition, a number of vertical measures have been adopted, applicable to specific type of content (terrorist content, child sexual abuse material, racist and xenophobic hate speech, intellectual property violations).

Figure 1: EU regulatory framework for online content moderation



Source: de Streel et al. (2020, p.19)

Out of all the legislations which were adopted or considered over the years at the EU level, the following are worth mentioning:

- **Directive combatting child sexual abuse materials** (2011) obliges Member States to take the necessary measures to ensure the prompt removal of, or with appropriate safeguards block access to, web pages containing or disseminating child pornography.⁴⁰ On that basis, Member States have implemented notice-and-takedown procedures through

³⁸ Points 16-21 of the Recommendation 2018/334.

³⁹ Points 22-28 of the Recommendation 2018/334.

⁴⁰ Directive 2011/93 of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography OJ [2011] L 335/1, art.25.

national hotlines which allow Internet users to report child sexual abuse material that they find online.⁴¹

- **Directive combatting terrorism** (2017) obliges Member States to take the necessary measures to ensure the prompt removal of, or with appropriate safeguards block access to, online content constituting a public provocation to commit a terrorist offence.⁴² In addition, a proposal for a **Terrorist Content Regulation** is currently being negotiated,⁴³ which covers preventive duties and the process of content removal of the terrorist content by the hosting providers.⁴⁴ It prescribes a removal of terrorist content within one hour.⁴⁵ It also includes rules concerning complaint mechanisms, transparency obligations and data retention.
- **General Data Protection Regulation (GDPR)** (2016) includes a special rule concerning search engines and their obligation to delist content from the search results (also known as 'right to be forgotten'). In addition, the new case-law of the Court of Justice gives providers data protection responsibilities concerning the hosted content under some circumstances.⁴⁶
- **Audiovisual Media Services Directive (AVMSD)** revised in 2018 regulates video-sharing platforms hosting content over which they do not have editorial responsibility, like user-generated content. It covers the protection of minors and the protection of the general public from incitement to violence and hatred, and from content that is illegal to disseminate such as terrorist, racist/xenophobic content, child pornography and illegal hate speech. Such platforms are obliged to take preventive measures concerning the organisation of the content and not the content as such. This includes measures like easy-to-use flagging systems, effective complaint systems, parental controls, age rating and age verification systems and transparency obligations.⁴⁷ Video-sharing platform providers are also responsible for ensuring that all commercial communication appearing on their platforms complies with the standards set out in the AVMSD,⁴⁸ including communication that is not marketed or sold directly by them. None of these measures may, however, lead to any ex-ante control measures or upload-filtering of content which do not comply with the prohibition of general monitoring measures of the ECD. Although Member States might adopt stricter preventive measures than those listed in AVMSD,⁴⁹ these are still subject to the same limitations of the ECD. In addition, the AVMSD includes some general requirements⁵⁰ concerning user's disputes over incorrect removal of content.
- **DSM Copyright Directive (DSMD)** adopted in 2019 regulates Online Content Sharing Service providers, like video- or picture-sharing platforms, and their responsibility for licensing of content posted by their users.⁵¹ By default, the providers have to engage in "best efforts" to obtain licenses for content potentially posted by their users. If such licenses are missing, though "best efforts" to obtain them can be demonstrated, they are liable for violation of copyright or neighbouring rights, *unless* they take down material upon notification and prevent its re-appearance on the service (given the relevant information in

⁴¹ Report from the Commission of 16 December 2016 assessing the implementation of the measures referred to in Article 25 of Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography, COM(2016) 872. INHOPE is the umbrella organisation for the hotlines.

⁴² Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism OJ [2017] L 88/6, art.21.

⁴³ Proposal of the Commission of 12 September 2018 for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, COM (2018) 640.

⁴⁴ See Article 3-6 of the Proposal.

⁴⁵ Article 4(2) of the Proposal.

⁴⁶ See Section 3.2; see on the relationship, Peguera M. (2016).

⁴⁷ AVMSD, art.28a(3). See Kukliš L. (2020).

⁴⁸ AVMSD, art. 9(1) and 28b(2)

⁴⁹ AVMSD, art.28a(6).

⁵⁰ AVMSD, art. 28a(3)(j);(7);(8).

⁵¹ Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market, OJ [2019] L 130/92

both cases).⁵² The preventive duties have to comply with the general monitoring prohibition, since Online Content Sharing Services Providers are of 'active' nature, although such obligation is an extension of Article 15 ECD requirement.⁵³ In addition, the DSMD includes a number of unspecified safeguards against incorrect removal of content by the providers which are absent in the ECD framework.

Furthermore, the European Commission encouraged self- and co-regulation in the area, such as:

- **Counterfeit goods** with the adoption of a *Memorandum of Understanding (MoU) on illegal counterfeiting* in 2011 between rights owners, Internet platforms and associations to improve notice-and-takedown, to enhance preventive measures taken by rights owners and online intermediaries, to increase cooperation and to fight better against repeated infringements. A revised version was signed in May 2016 to include Key Performance Indicators in order to facilitate its monitoring.⁵⁴
- **Child sexual abuse materials** with the establishment of the *Alliance to Better Protect Minors Online* in 2017 composed of actors from the entire value chain (devices manufacturers, telecoms, media and online services used by children) to address emerging risks that minors face online, such as harmful content (e.g. violent or sexually exploitative content), harmful conduct (e.g. cyberbullying) and harmful contact (e.g. sexual extortion).⁵⁵
- **Terrorist content** with the establishment of a *Multi-Stakeholders Forum* in 2015 between the EU Interior Ministers, the major internet companies (such as Facebook, Google, Microsoft and Twitter), Europol, the EU Counter Terrorism Co-ordinator and the European Parliament to address the misuse of Internet by terrorist groups and to reduce accessibility to terrorist content online.⁵⁶ The Forum led to an efficient referral mechanism in particular by the EU Internet Referral Unit of Europol, a shared database of hashes with more than 200,000 hashes of terrorist videos and images.
- **Hate speech** with the adoption of an *EU Code of Conduct on countering illegal hate speech online* in 2016 that has since been adopted by major and mid-sizes online content platforms (namely Facebook, Microsoft, Twitter, YouTube, Instagram, Dailymotion, Snapchat, TikTok and Jeuxvideo);⁵⁷
- **Online disinformation and fake news:** with the adoption of a *Code of Practice on Disinformation* in 2018 by four online platforms (Facebook, Google, Twitter, and Mozilla), advertisers and the advertising industry.⁵⁸ It was also adopted later by Microsoft and TikTok.

⁵² DSMD, art.17(4).

⁵³ See on the reason why active services are not covered by Article 15 ECD in Section 2.2.3.

⁵⁴ See https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en

⁵⁵ See <https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online>. For an evaluation of such Alliance, see Ramboll (2018). Previous initiatives were: a CEO Coalition in 2011: 'Self-regulation for a Better Internet for Kids' <https://ec.europa.eu/digital-single-market/en/self-regulation-and-stakeholders-better-internet-kids>; an ICT Coalition for Children Online in 2012: <http://www.ictcoalition.eu>.

⁵⁶ Commission Press release of 3 December 2015, IP/15/6243.

⁵⁷ Code of Conduct of May 2016 on countering illegal hate speech online: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300.

⁵⁸ Code of Practice on Disinformation", 26 September 2018, last updated 17 June 2019, available at: <https://ec.europa.eu/digital-single-market/en/news/Code-practice-disinformation>. The Code of Practice is regularly assessed by the Commission. See also the evaluation done by ERGA (2020) and VVA (2020).

Table 1: Main EU rules against illegal content online

Type of illegal content	Hard-law	Soft-law	Self-regulation
<p>BASELINE</p> <p>All types of hosting platforms and all types of illegal content online</p>	<p>- Directive 2000/31 on e-Commerce</p>	<p>- Communication (2017) on Tackling <i>Illegal Content Online</i></p> <p>- Commission <i>Recommendation 2018/334</i> on measures to effectively tackle illegal content online</p>	
<p>Additional rules for Video-Sharing Platforms</p>	<p>- Directive 2010/13 Audiovisual Media Services as amended by Directive 2018/1808</p>		
<p>Terrorist content</p>	<p>- Directive 2017/541 on combating Terrorism</p> <p>- Proposal Regulation on preventing the dissemination of preventing the dissemination of terrorist content online</p>	<p>- Commission <i>Recommendation 2018/334</i> on measures to effectively tackle illegal content online</p>	<p>- EU Internet Forum (2015)</p>
<p>Child sexual abuse material</p>	<p>- Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography</p>		<p>- Alliance to Better Protect Minors Online (2017)</p>
<p>Illegal hate speech</p>	<p>- Council Framework Decision 2008/913 on combating certain forms and expressions of racism and xenophobia</p>		<p>- Code of Conduct on illegal hate speech online (2016)</p>
<p>Intellectual property violation</p>	<p>- Directive 2019/790 on Copyright in the Digital Single Market</p> <p>- Directive 2004/48 on enforcement of Intellectual Property Rights</p>		<p>- Memorandum of Understanding on counterfeit goods online (2011, rev. 2016)</p>

Source: de Streel et al. (2020, p.33)

4.2 Critique and shortcomings of the liability regime

In the context of developing the online platform strategy in 2016-2017, the **Commission evaluated the liability regime of the ECD** based on a series of public consultations⁵⁹ and independent studies. According to the 2016 Commission public consultation,⁶⁰ '[a] majority of the respondents stand behind intermediary liability principles of the E-Commerce Directive, but also demands some clarifications or improvements'. A significant proportion of respondents who criticized the Directive complained about the national implementations rather than the EU law itself. The stakeholders broadly supported the horizontal nature of the Directive, but demanded a differentiated approach on Notice-and-action by adjusting or improving the practice of take-down for specific types of content, such as hate-speech, terrorist content, child abuse material, copyright infringements, etc.

Regarding the functioning of ECD rules, the hosting safe harbour drew the most attention (Article 14), specifically the concepts and the distinction between active and passive hosting. The distinction was criticized for not being entirely clear, and for the divergent interpretations of the article within Member States. As regards the missing components, an '[o]verwhelming majority of respondents supported the establishment of a counter-notice mechanism (82.5%), i.e. possibility for content providers to give their views to the hosting service provider on the alleged illegality of their content'.⁶¹ The consultation also recorded significant support for more transparency on the intermediaries' content restriction policies.⁶² On the side of preventive duties, a majority of intermediaries reported that they do put in place voluntary or preventive measures to remove certain categories of illegal content from their system beyond what was required by the legal framework. In the consultation, only 36.1% of respondents reported a need to impose specific duties of care for certain categories of content.

In the academic literature, de Streef and Husovec (2020, p. 39) explain that **empirical studies looked at the question of removing illegal content**. However, most of them are copyright-centred, and not necessarily localised to only EU markets. Those studies of the ecosystem fit into several categories: (i) interviewing notifiers, providers and users;⁶³ (ii) experimental upload of content,⁶⁴ (iii) analysis of transparency reports or data sets shared publicly by providers, such as *Lumen* data⁶⁵, (iv) tracking the public availability of the content over a pre-set period⁶⁶ and (v) experimental testing of redesigns of ECD.⁶⁷ The studies so far show a number of global trends, which are not always localized to the European setting, namely:

- the quality of notifications sent to the providers is often low (at least in some areas);
- there is a diverging quality of such notifications among different notifiers;
- the notifications are increasingly out-sourced to professional companies;
- the notifications are increasingly sent by algorithms, and not humans;
- providers tend to over-remove content to avoid liability and save resources;
- they equally employ technology to evaluate the notifications;
- the affected users who posted content often do not take action.

On the basis of the evaluation and academic studies, de Streef and Husovec (2020, pp. 41-44) summarise the main criticism of the Directive's liability rules as follows:

⁵⁹ The results of the public consultation could be found at: <https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud>. For an qualitative analysis of the results, see TILT (2016).

⁶⁰ TILT (2016, p. 4).

⁶¹ Ibid, p. 5.

⁶² Ibid, p. 6.

⁶³ Urban et al. (2017a)

⁶⁴ Perel and Elkin-Koren (2017); Sjoera (2004).

⁶⁵ Urban et al. (2017a) and (2017b); Seng (2014) and (2015); See www.lumendatabase.org.

⁶⁶ Erickson and Kretschmer (2018).

⁶⁷ Fiala and Husovec (2018).

(1) The **Directive lacks any safeguards to prevent violations of fundamental rights**, notably freedom of expression. The ECD does not include provisions which would provide for effective and tested mechanisms to avoid and/or resolve incorrect removals of content. This lack of safeguards leads to over-notification by notifiers, over-removal by providers and under-assertion of rights by affected users. Empirical evidence confirms the aforementioned phenomena. Although some recent sectorial initiatives like AVMSD and DSMD include safeguards, even these are arguably very vague.

The potential measures suggested in the literature include carrots and sticks for all these stakeholders in the enforcement chain. In order to work, they need to be scalable. For notifiers, potential measures include fines or processing penalties (e.g. delays or suspension of automated submission possibilities for low-quality notifiers) in case of low-quality notifications, enhanced access for notifiers who have a proven record of notification quality. For providers and affected users, potential measures include transparency to the public and obligation to explain the decisions to affected users, obligatory human review, internal and external dispute mechanism, judicial remedies against providers, and fines for high numbers over-removals.

(2) The **Directive does not envisage that notifications may be sent by robots** rather than humans, and fails to incentivize the quality of sent and reviewed notifications. This criticism is connected with the previous one. Empirical studies document that automation of notifications is responsible for their rise. ECD assumed that notifications are sent by humans, which is clearly outdated. Moreover, we see a rise of outsourcing notification activity to professional service providers, like law firms or enforcement agencies.

(3) The **ECD does not prevent fragmentation caused by diverging application of the passivity criterion by the national courts**. The stakeholders obviously disagree about the correct scope of passive/active criterion. The passivity criterion is responsible for some divergence in the case-law concerning the hosting safe harbour⁶⁸ and that it discourages rather than encourages more preventive measures. The criterion is a reason why some of the national courts avoid application of the ECD framework (as active services are out of the scope). To facilitate harmonization, several authors suggest either to abandon the criterion for hosting or to clarify it.⁶⁹ Same demands surfaced from the 2016 Commission consultation. The main policy concern behind the passivity criterion is that it potentially *discourages* voluntary preventive measures by the providers (at least in some Member States), who might be afraid to lose their safe harbours if they take those preventive measures (so called 'good Samaritan paradox'). This is obviously counter-productive, because the ECD in essence aims to incentivize more preventive actions to be taken by providers.

(4) The **Directive failed to include hyperlinking and search engines and it does not cover other new services either**. As a consequence, it has been criticized for missing out on socially valuable services.⁷⁰ Other examples of services which are not covered include domain name authorities, domain registrars, online payment services and autocomplete or autosuggestion services. Some of these services were rarely targets of litigation, others were more often.

(5) The **Directive only serves as a limit and not as a comprehensive tool for removal of illegal content**. Because the Directive only provides for a broad framework, the Member States can establish different rules under its umbrella.

First, the Directive creates a legal basis neither for reactive removal (as it does not ever establish liability), nor for specific duties (e.g. to terminate accounts for repeated illegal uploads). Hence, Member States have foreseen different notice and takedown processes for hosting services.⁷¹ This creates a challenge for the Digital Single Market as notifications, removals and complaints cannot

⁶⁸ van Hoboken et al. (2018).

⁶⁹ Angelopoulos (2016); Husovec (2017).

⁷⁰ See van Hoboken (2009).

⁷¹ As explained in ICF, Grimaldi and 21c (2018).

be simply scaled across the EU. They can have different systems of specific preventive or corrective duties.

Second, the importance of the EU framework might differ across the Member States given that the consequences following the loss of a safe harbour can be of a different magnitude. For instance, losing a hosting safe harbour in one country could immediately lead to liability, while in others any liability might require further conditions to be met. This complicates private and public enforcement.

Third, the lack of specificity of the Directive allows bad actors to escape good practices when implementing the notice and takedown system. Two countries thus can have very different experiences with the same type of policy because they regulated the process of knowledge acquisition and the subsequent response differently. To address these challenges, some commentators propose more detailed rules, in line with the Commission Recommendations, which would define the process on the EU level.⁷²

4.3 Reforming the baseline regime: strengthening procedural accountability

The baseline liability regime contained in the ECD could be amended by appropriately and proportionately strengthening the responsibility of online platforms in order to ensure safer digital services. The new rules could include a **set of fully harmonised rules on procedural accountability to allow public oversight on the way in which platforms moderate content**.⁷³ These rules could make sure that platforms abide by good governance rules and practices which reflect EU democratic and fundamental right values. They could ensure oversight of policies, processes and tools put in place by platforms to ensure that illegal content is taken down where needed. To remain proportionate, smaller platforms could need to abide by the same set of procedural rules tailored according to their size, type and reach.

Those rules on procedural accountability could relate to the 'notice-and-takedown' procedure to facilitate reporting by users, to the possibility and the need to take proactive measures to facilitate platforms' detection and to the cooperation with public enforcement authorities. They could be based on the measures put down by the European Commission in its Recommendation to effectively tackle illegal online content as well as on the measures imposed on Video-Sharing Platforms by the revised Audiovisual Media Services Directive⁷⁴. In other words, it could integrate some soft-law recommendations into the hard-law and extend the rules currently applicable to VSPs to all online content platforms.

Importantly, **different obligations should be imposed for harmful content** than for illegal content as freedom of speech needs to be preserved. Relevant measures could include: closing false accounts and fighting bots; promoting independent counter-speech and relevant, authentic and trustworthy content (e.g. from experts); encouraging finding alternative content on general interest content; strengthening transparency measures, media literacy and democracy education; and making parental control tools and rating systems available.

4.3.1 Increased role for users and trusted flaggers

The forthcoming DSA with the expected revision of the ECD could introduce more expansive rules on **transparency concerning content removal**, their processing, mistakes, actors and notifications. Such rules could also ensure personalised explanations for affected users and audits for authorities or researchers⁷⁵.

Providers of hosting services could set up mechanisms for notices that are easy to access, user-friendly and allow for automated submission. The **'notice-and-takedown' system could be**

⁷² Kuczerawy (2018); Buiten, de Streel and Peitz (2020).

⁷³ Wood and Perrin (2019) propose to impose a duty of care on online platform but Nash (2019) suggest procedural accountability.

⁷⁴ Commission Recommendation 2018/334, 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: <https://www.santaclaraprinciples.org/>.

⁷⁵ As recommended by the High-Level Expert Group on Artificial Intelligence (2019).

facilitated and based on common principles defined at EU level⁷⁶. Husovec (2018) suggests to only legislate the essential requirements of the process and then leave the details to the standardisation process at the European Standards Organisations (CEN, CENELEC and ETSI), which can better reflect industry-wide best practices in different areas. Such technical standards could then serve as a proof of the provider's best efforts to comply with the 'notice-and-takedown' system as diligently as possible⁷⁷. Technical standardisation could better foresee and keep up with automation, new techniques used and other market developments.

To reduce the risks of type I errors (over-removal) and ensure an appropriate balance among fundamental rights, the platform could⁷⁸:

- encourage **notices** that are sufficiently precise and adequately substantiated;
- when practical and proportionate, first inform the content provider of the intention to suspend access to the suspect material and of the reason of such suspension, and give the provider the possibility to contest such suspension by submitting a '**counter-notice**'; and
- the platform could only remove the material from all platforms active in the EU after having assessed in a diligent manner, on the basis of the information given, the validity and the relevance of this 'counter-notice'.

However, in exceptional circumstances, when the illegality manifests and relates to serious criminal offences involving a life threat or safety of persons (such as terrorist content), content may be removed immediately.

Online platforms could also cooperate more closely with hotlines and **trusted flaggers** that could be designated by clear and objective criteria based on expertise. Such cooperation may lead to fast-track procedures for notices submitted by trusted flaggers.⁷⁹

4.3.2 Preventive measures

Where appropriate, certain online platforms could be **encouraged to take proportionate and specific proactive measures** in respect of illegal online content, even by automated means.⁸⁰ However, some safeguards could be in place and such proactive measure could not lead to a general monitoring that should continue to be prohibited.

A '**Good Samaritan**' clause could be affirmed explicitly to ensure that the online platforms taking on proactive measures are not treated in a less favourable way than the ones not taking these measures.⁸¹ Such 'Good Samaritan' clause could aid platforms when taking voluntary measures by removing the risk of being sanctioned for under-removal.

Reliance on **automated detecting tools** by intermediaries or users could be encouraged as an effective detection means, provided some safeguards be in place. This is part of the wider debate on the EU Regulation of Artificial Intelligence (AI), which should be based on the application of six key requirements: human agency and oversight; technical robustness and safety; privacy and data governance; transparency, diversity, non-discrimination and fairness; societal and environmental wellbeing; and accountability.⁸² Moreover, there may be a need for the large online platforms (which

⁷⁶ Also Husovec (2017), Sartor (2017).

⁷⁷ This is similar to the so-called "New Approach" used by the EU since the eighties in the field of technical standardisation and product safety and security.

⁷⁸ Commission Recommendation 2018/334, Points 5-13; AVMSD, Article 28b(3) (d)-(e).

⁷⁹ Commission Recommendation 2018/334, Points 25-27.

⁸⁰ Commission Recommendation 2018/334, Points 18-20.

⁸¹ Also in this sense, Sartor (2017:29). As already explained, the European Commission considers that the 'Good Samaritan' clause is already compatible with the e-Commerce Directive: Communication on tackling illegal online content, COM(2017), p.13.

⁸² European Communication White Paper of 19 February 2020 on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65; High-Level Expert Group on Artificial Intelligence, Ethics Guidelines of 8 April 2019 for Trustworthy AI. Explainability obligations already imposed by the GDPR and other recent EU laws apply to automated content moderation practice. On these obligations and their technical implementation, see Bibal, Lognoul, de Streel and Frenay (2020).

have the data, the expertise and the financial means to develop automated techniques) to **share these technologies** with the small and medium-sized or new platforms,⁸³ as is already the practice in efforts to combat child sexual exploitation and terrorist content.

4.4 Aligning responsibility with risks

In addition to reforming the baseline regime applicable to all categories of platforms and all types of content, stricter rules increasing the responsibility of the platforms should be imposed when the risks of online harms also increase.⁸⁴ **To reflect such risk-based approach, differentiation could be made** according to:

- The type of online content: more extensive obligations could be imposed on the moderation of the illegal content with the highest negative impact on society. This is already the case today as stricter rules are imposed against terrorist content, child sexual abuse material, racist and xenophobic hate speech. All those rules should, on the one hand, be coherent with each other and with the baseline regime and, on the other hand, provide sufficient and effective safeguards to ensure appropriate balance among fundamental rights set by the Court of Justice of the EU and the European Court of Human Rights.
- The **size of the online platform: more extensive obligations could be imposed on the platforms with the largest size**. Thanks to their innovation, some content-sharing platforms have become so large and so important in the life of citizens that they are not merely running a private space anymore but hosting part of the public space.⁸⁵ Such differentiation by platforms size is already emerging in EU law but should be affirmed more clearly in the forthcoming DSA.

In practice, platforms with a number of users above a certain threshold that could be designated as **Public Space Content-Sharing Platforms (PSCSPs)** could be subject to more extensive procedural accountability obligations. They could also be required to adopt regular transparency reports explaining how they moderate content with clear and comparable statistics. Also, to increase the incentive to comply with those rules, the liability exemption of the ECD could be conditioned for PSCSPs to comply with stricter procedural accountability obligations. In other words, if a PSCSP does not set up an appropriate 'notice-and-takedown' mechanism or does not take appropriate proactive measures, the platform would not be able to rely on the liability exemption provided in the ECD. In addition, as explained in the following section, those PSCSP could also be subject to a differentiated oversight and be supervised by an EU authority and not the authority of the Member State where the PSCSP is established.

5 Improving oversight and enforcement

5.1 Existing rules

First, the ECD sets some **safeguards about the national enforcement mechanisms** to ensure their effectiveness. The sanctions in case of violation of the ECD rules should be effective, proportionate and dissuasive.⁸⁶ Furthermore, the available national court actions should be effective allowing for the rapid adoption of corrective measures, including interim measures.⁸⁷

Second, the ECD encourages **cooperation and mutual assistance between Member States and with the Commission** for the implementation of the rules on ISS, in particular through the establishment of national contact points.⁸⁸ Given the application of the 'country of origin' principle,

⁸³ Commission **Recommendation 2018/334**, Point 28.

⁸⁴ For a law and economics approach of the liability rules of online platforms, see Buiten, de Streef and Peitz (2020).

⁸⁵ As suggested by Smith (2020), those public space platforms should now be regulated according to public law values and not anymore according to private law values.

⁸⁶ ECD, art.20.

⁸⁷ ECD, art.18.

⁸⁸ ECD, art.19.

it is key to have an effective cooperation between the Member State where the ISS provider is established and regulated and the Member State of destination where the ISS is offered. The ECD also provides procedural conditions if the Member State of destination wants derogate to the country of origin principle and regulate the provider of ISS.⁸⁹

Third, the ECD encourages the reliance on **alternative enforcement modes** such as conclusion of Codes of conduct at the EU level⁹⁰ or out-of-court dispute settlement schemes.⁹¹

The **use of self- and co-regulation** tools may be justified when technology and market evolve quickly and the asymmetry of information between the stakeholders and the authorities is high. In this case, it may be difficult, if not impossible, for the legislator to impose the appropriate obligations and remedies. Indeed, we have seen that Code of Conducts were very much encouraged by the Commission to limit the spread of harmful or illegal content and material online. However, there is an obvious risk that self-regulation is self-serving⁹² and/or is not well enforced. Therefore, Codes of conduct should comply with the principles for better self- and co-regulation proposed by the Commission.⁹³ Those principles ensure that rules are prepared openly and by as many relevant actors representing different interests and values as possible, and they are monitored in a way that is sufficiently open and autonomous and are sanctioned when violated.⁹⁴

On the **Code of Conduct on hate speech**, commentators have pointed towards the following weaknesses⁹⁵: (i) risks of private censorship practices through the priority application of Community Standards/Guidelines; (ii) lack of precision in determining the validity of a notification; (iii) absence of appeal mechanisms for users whose content has been withdrawn; (iv) illegal content does not have to be reported to the competent national authorities when removed on the basis of the Community Standards/Guidelines; and (v) the 24-hour deadline could either make it impossible for online platforms to meet their commitments or lead them to over-blocking practices.

On the **Code of Practice on online disinformation**, the European Regulators Group for Audio-Visual Media Services (ERGA, 2020) notes (i) a need for greater transparency on the implementation of the Code with a mechanism to ensure independent verification of information provided; (ii) the overly general nature of the commitments (both in terms of content and structure); and (iii) the need to increase the number of signatories, in particular to include all the big platforms. ERGA believes that improving the effectiveness of the Code requires that all online platforms must uniformly comply with the same obligations and that more precise definition, procedures and commitments need be adopted. ERGA calls for a shift from self-regulation to co-regulation to enhance the effectiveness of the fight against online disinformation. In an Evaluation Study done for the European Commission, VVA (2020) analyses the Terms of Service/Use and Community Standards/Guidelines that online platforms have implemented to comply with the Code of Practice. The study makes three main criticisms: (i) given its self-regulatory nature, it is not possible to force signatories to comply with their commitments and they do not cover all stakeholders; (ii) implementation of the commitments across the different online platforms, pillars and Member States is fragmented; and (iii) the scope and the key concepts of the Code of Practice lack clarity. In this respect, VVA suggests the adoption of a common terminology among signatories and that the actions undertaken should be as concrete as possible. This would make it easier to implement and monitor the commitments and to define expected results and key performance indicators.

VVA also recommends strengthening the effectiveness of the Code of Practice by running more debates on the strengths and weaknesses of the Code, by establishing mechanism for sanctions and

⁸⁹ ECD, art. 3(4b).

⁹⁰ ECD, art. 16.

⁹¹ ECD, art. 17.

⁹² As argued in Smith (2020). Also Bartle and Vass (2007).

⁹³ Those principles are available at: <https://ec.europa.eu/digital-single-market/en/best-practice-principles-better-self-and-co-regulation>.

⁹⁴ See also, Finck (2018).

⁹⁵ Coche (2018); Quintel and Ullrich (2019).

redress in case of non-compliance with the commitments in the Code/ Moreover, co-regulation should also be considered.

For the oversight of video-sharing platforms, the AVMSD requires **national regulatory authorities to engage in regular monitoring** of the measures that platforms take in order to protect users. This is done by the authority in the country of origin, with detailed instructions for determining jurisdiction set out in the Directive. In addition, the AVMSD facilitates coordination among national regulators through the formalisation of the role of ERGA and elaboration of a coordination process. Similar **coordination takes place among self-regulatory organisations to advertise enforcement of national Codes of conduct** through the European Advertising Standards Alliance (EASA), though without Commission involvement. EASA operates a cross-border complaints mechanism for handling potential code violations across jurisdictions. Although advertising Codes are national level Codes rooted in national cultural and economic contexts, they already apply to online advertising and are generally based on the Code developed by the International Chamber of Commerce, which reflects the requirements related to advertising standards contained in the AVMSD.

The **use of alternative dispute resolution**, more importantly online, may also be justified when disputes are many and could be easily solved, possibly with the help of automated tools. Indeed, as explained above, there is increasing automation in the detection and the removal of illegal content online. However, it is important that fundamental rights, in particular due process, are respected and that the last word on possible balance between fundamental rights is left to the courts of the Member States and the EU.

5.2 Avenues for reforms

5.2.1 Enforcement with public authorities

- *Public enforcement by independent authorities*

The online platforms should be **supervised by the authorities of the country where they are established** according to the 'country of origin' principle. These authorities should be fully independent given the importance of their role in upholding freedom of expression, media plurality and press freedom. Minimum expectations for independence for national regulators have been outlined in article 30 of the AVMSD. Moreover, the **cooperation and mutual assistance between Member States should be strengthened**, in particular between the country of origin where the online platform is established and the country of destination where the platform is offering its services.

However, the authorities of the country of establishment may not have either the ability or the incentive to regulate the largest online content platforms, referred to as the Public Space Content Sharing Platforms which could be subject to stricter moderation obligations as explained above. For those platforms, EU rules **could be enforced by an independent EU regulator** - in close partnership with the national regulatory authorities - which would be sufficiently funded to conduct investigations into the operation of platforms as well.⁹⁶ Moreover, the EU independent authority could also maintain a database of which national authority is in charge of which platform and deal with ones that have no EU country of origin.

- *Private enforcement*

Where a moderation practice breaches the rights of users in at least two EU countries other than the EU country where the infringement originated or for widespread infringements, **the mechanism set up under the EU Consumer Protection Cooperation Network Regulation could come into play**. According to this Regulation, national authorities should give a coordinated response to

⁹⁶ In that regard, the enforcement of financial regulation on systemic banks by Single Supervisory Mechanism within the European Central Bank is an interesting good practice: Council Regulation 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions, O.J. [2013] L 287/63.

cross border infringements of EU consumer protection legislation through a network that has been established among them. For instance, the Consumer Protection Cooperation Network adopted a common position on stopping scams and unfair business practices on online platforms in the context of the COVID-19 outbreak.⁹⁷ Progressively, the mechanism has been broadened to cover breaches of a wide range of EU legislative instruments, which are no longer necessarily linked to consumers per se, such as breaches of the AVMSD.

5.2.2 Enforcement with private bodies

- Codes of Conduct, self- and co-regulatory bodies

Codes of Conduct should continue to be encouraged as they can be very useful in fast moving industries where the best manners to achieve regulatory goals set in the law are not easy to determine. However, given their increasing importance, the DSA could impose **additional safeguards** in such a manner that Codes are established and monitored in order to increase their legitimacy, their effectiveness and compliance with fundamental rights, thus leading to a co-regulatory approach. In particular, the DSA could follow the line taken in the AVMSD that implies codes of conduct 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.⁹⁸

Moreover, as in the German NetzDG, the possibility of using a **self-regulatory body, recognised by the State to rule on the illegality of online content** (when it is not unquestionably illegal) could be explored in order to alleviate the risk of over-removal. This mechanism has just been put in place in Germany so there are still lessons to be learned. However, the approach is attractive as it could discharge platforms from taking difficult decisions, while giving users certain safeguards and alleviating the possible incentives of platforms to over-removal out of fear of heavy fines and therefore prefer to remove content that is legal in case of doubt.

- Out-of-Court dispute resolutions mechanisms

Dispute resolution is of fundamental importance as users need to be able to challenge decisions by platforms 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.

In that regard, Fiala and Husovec (2018) propose to create an external ADR, which would be financed by higher fees paid by providers that erroneously take down the content and lower fees by users who complain without success. Such fees are meant to incentivise providers to improve their internal processes and provide a credible remedy for users to get their content reinstated and be heard by an impartial body.⁹⁹

⁹⁷ The common position is available at:

https://ec.europa.eu/info/sites/info/files/live_work_travel_in_the_eu/consumers/documents/cpc_common_position_covid19.pdf.

⁹⁸ See AVMSD, new Article 4a introduced by Directive 2018/1808.

⁹⁹ The authors note that in the laboratory experiments, the solution mitigates the over-removal and increases legitimate complaints by users. An important implementation requirement would be, however, that providers would have to be bound by these ADR decisions at least for some limited time in order to prevent circumvention through changes of terms of service. Otherwise, there is risk that each ADR decision can be instantly circumvented by providers through a simple change in terms of the service. Since the value of user's content usually goes down with passing time, introducing delay to such changes should be sufficient for users to protect their speech interests, while assuring that providers control the 'house rules'.

6 References

Angelopolous C. (2016), *European Intermediary Liability in Copyright: A Tort-Based Analysis*, Information Law Series Volume 39, Kluwer.

Bibal A., M. Lognoul, A. de Streeel and B. Frenay (2020), "Implementing Legal Requirements on Explainability in Machine Learning", *Artificial Intelligence and Law* 28,

Buiten M., A. de Streeel A and M. Peitz (2020), Rethinking Liability Rules for Online Hosting Platforms, *International Journal of Law and Information Technology* 28, 139-166.

Bartle I. and P. Vass (2007), 'Self-regulation within the Regulatory State', 85 *Public Administration*, 885-905.

Cappello M. (ed.), *Self- and Co-regulation in the new AVMSD*, IRIS Special, European Audiovisual Observatory.

de Streeel A., A. Kuczerawy and M. Ledger (2019), 'Online Platforms and Services', in L. Garzaniti et al (eds), *Electronic communications, Audiovisual Services and the Internet: EU Competition Law and Regulation*, 4th ed., Sweet & Maxwell, 125-157.

de Streeel A. and M. Husovec (2020) The e-Commerce Directive as the cornerstone of the Internal Market: Assessment and Options for Reforms, Study for the European Parliament.

de Streeel A. et al. (2020), *Online Platforms' Moderation of Illegal Content Online*, Study for the European Parliament.

Erickson K. and M. Kretschmer (2018) 'This Video is Unavailable: Analyzing Copyright Takedown of User Generated Content on YouTube', 9 *Jour. of Intellectual Property, Information Technology and Electronic Commerce Law* 75.

ERGA (2020) *Report on disinformation: Assessment of the implementation of the Code of Practice*, available at: <https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf>.

Fiala L and M. Husovec (2018), 'Using Experimental Evidence to Design Optimal Notice and Takedown Process', *TILEC Discussion Paper 2018-028*.

Finck M. (2018) 'Digital co-regulation: designing a supranational legal framework for the platform economy', 43 *European Law Review* 47-68.

Floridi L. and M. Taddeo (2017). *The responsibility of Online Service Providers*, Springer.

Helberger N., J. Pierson and T. Poell (2018), "Governing online platforms: From contested to cooperative responsibility", *The Information Society* 34(1), pp. 1-14.

Husovec M. (2017), *Injunctions Against Intermediaries in the European Union : Accountable But Not Liable?*, Cambridge University Press.

Husovec M. (2018), The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown? Which is Superior? And Why?, 42(1) *Columbia Journal of Law & the Arts*, 53-84

ICF, Grimaldi Studio Legale, and 21c Consultancy (2018), *Overview of the legal framework of notice-and-action procedures in Member States*, Study for the European Commission.

Kuczerawy A. (2018), *Intermediary Liability and Freedom of Expression in the EU: from Concepts to Safeguards*, Intersentia.

Kukliš L. (2020), "Video-Sharing Platforms in AVMSD – A new kind of content regulation", *Research Handbook on EU Media Law and Policy*, Elgar Publishing.

Mahieu R., J. van Hoboken and H. Asghari (2019) 'Responsibility for Data Protection in a Networked World – On the Question of the Controller, 'Effective and Complete Protection' and Its Application to Data Access Rights in Europe', 10 *Jour. of Intellectual Property, Information Technology and Electronic Commerce Law*, 39.

Martens B. (2016), "An Economic Policy Perspective on Online Platforms", *JRC Technical Report, Digital Economy Working Paper 2016/05*.

Nash V. (2019). "Revise and resubmit? Reviewing the 2019 Online Harms White Paper". *Journal of Media Law*, 11:1, pp. 18-27.

Nordermann J.B. (2018), *Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?*, In-depth analysis for the IMCO Committee of the European Parliament.

Nordermann J.B. (2020), The functioning of the Internal Market for digital services: Responsibility and duty of care of providers of digital services, In-depth analysis for the IMCO Committee of the European Parliament.

Peguera M. (2009a), 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems' 32 *Columbia Journal of Law & the Arts*, 481.

Peguera M. (2009b), 'When the Cached Link is the Weakest Link: Search Engine Caches under the Digital Millennium Copyright Act', 56 *Journal Copyright Society of the U.S.A.*, 589.

Peguera M. (2016), The Shaky Ground of the Right to Be Delisted, 18 *Vanderbilt Journal of Entertainment & Technology Law* 507.

Perel, M and N. Elkin-Koren (2017), Black box tinkering: Beyond transparency in algorithmic enforcement, 69 *Fla. L. Rev.* 181

Ramboll (2018), Evaluation of the implementation of the Alliance to Better Protect Minors Online, Study for the European Commission.

Sartor G. (2017), *Providers Liability: From the eCommerce Directive to the future*, In-Depth Analysis for the IMCO Committee of the European Parliament.

Seng D. (2014) 'The state of the discordant union: An empirical analysis of DMCA takedown notices' 18 *Va J L & Tech* 369.

Seng D. (2015), 'Who Watches the Watchmen?' An Empirical Analysis of Errors in DMCA Takedown Notices', available at SSRN.


Sjoera, N. (2004). The multatuli project isp notice and take down. <https://www-old.bof.nl/docs/researchpaperSANE.pdf>

Smith M. (2020), Enforcement and cooperation between Member States: E-Commerce and the future Digital Services Act, In-depth analysis for the IMCO Committee of the European Parliament.

TILT (2016), Role of online intermediaries: Summary of the public consultation, Study for the European Commission.

Urban, J.M, J. Karaganis and B.L. Schofield (2017a), "Notice and Takedown: Online service provider and rightholder accounts of everyday practices", *Journal of Copyright Society* 64, pp. 371-410.

Urban J.M, B.L. Schofield and J. Karaganis (2017b), "Takedown in Two Worlds: An Empirical Analysis", *Journal of Copyright Society* 64, 483-520.



Van Eecke P. (2011), 'Online Service Providers and Liability: A Plea for a Balanced Approach', *Common Market Law Review* 48, 1455-1502.

van Hoboken J. (2009), Legal Space for Innovative Ordering: On the Need to Update Selection Intermediary Liability in the EU, 13 *International Journal of Communications Law & Policy*.

van Hoboken J., J. Pedro Quintais, J. Poort and N. van Eijk (2018), *Hosting Intermediary Services and Illegal Content Online*, Study for the European Commission.

VVA (2020), Assessment of the implementation of the Code of Practice on Disinformation, Study for the European Commission.

Wood L. and W. Perrin (2019). *Online harm reduction – a statutory duty of care and a regulator*, Carnegie UK Trust, available at:

https://d1ssu070pg2v9i.cloudfront.net/pex/carnegie_uk_trust/2019/04/08091652/Online-harm-reduction-a-statutory-duty-of-care-and-regulator.pdf



WORKSHOP DISCUSSION SUMMARY

WORKSHOP DISCUSSION SUMMARY

The purpose of this section is to list the questions and discussion points that arose from the overview presented in the Issue Paper and the exclusive workshop organised in October 2020.

Clarifying responsibilities for a safer Internet

How can the **baseline liability regime**, applicable to all online platforms and for all illegal content, be improved?

Should procedural accountability be strengthened?

Should the rules provided in the 2018 Commission Recommendation on tackling illegal content be included in a hard-law instrument?

Should the content moderation and protection measures outlined in the revised AVMSD for video-sharing platforms be generalised for all types of online platforms?

RESPONSES

When developing new forms of procedural accountability applicable to online platforms, measures imposed by the revised Audiovisual Media Services Directive (AVMSD) on video-sharing platforms are seen as a good basis, as long as the measures do not become too prescriptive, and remain principle-based and neutral regarding the type of services and new services coming into the market. There needs to be a good mixture of quantitative and qualitative assessments by the regulator when it comes to accountability.

Should the **notice and takedown system** be harmonised at the EU level, at least partly?

Should a technical harmonisation of the system within Standard Setting Organisations be encouraged or imposed?

RESPONSES

There are currently 27 different Member States' regimes for hosting services of 'notice and takedown' mechanisms. Such fragmentation for notifications, removals, and complaints presents a real challenge for the Digital Single Market. From a practical point of view, harmonisation across the EU would be strongly welcomed, especially to help smaller platforms grow their presence across the EU, rather than just focusing on their home markets.

Concerning possible technical harmonisation of the system within Standard Setting Organisations (such as CEN, CENELEC, and ETSI), there is some level of scepticism around the use of standardisation for online content, mainly because of the long process and procedural work usually required for setting standards within those Organisations. The static nature of standards is also criticised, because of the lack of flexibility and agility to be compatible with the rapid development of new technologies in the online domain.

Some participants suggest taking a step back instead and looking at how standards such as content moderation standards were designed in the first place, as opposed to focusing on the standardisation process itself.

Should the online platforms be incentivised to take more **proactive/preventive measures** while respecting fundamental rights?

How this could be achieved?

Through a "good Samaritan" clause and other reforms?

RESPONSES

Although the current distinction between active and passive platforms (as mentioned in article 14 of the ECD) is encouraged to be taken further into account in the design of future regulatory proposals, this distinction potentially discourages voluntary preventive measures by the providers (at least in some Member States), who might be afraid to lose their safe harbours if they take preventive measures. Clarification of the criteria for passive and active hosting platforms would be welcome.

Consideration could be given to a "duty of care" for companies that facilitate the sharing of user-generated content, as mentioned in the UK White Paper on Online Harms published early 2020, and already used in the financial sector. Companies would then need to have effective, accessible complaints and reporting mechanisms for users to raise concerns about specific pieces of harmful content.

A "good Samaritan" clause could also ensure online platforms taking on proactive and voluntary measures are not treated less favorably than the ones not taking any measures by removing the risk of being sanctioned for under-removal.

Which obligations should be imposed to effectively monitor effectiveness and compliance with fundamental rights in case of reliance on **automated tools** to moderate the online content?

RESPONSES

The above question looks at Human Rights as a safeguard that limits the use of automated tools. Focus should instead be on how to apply fundamental rights in the first place, i.e. at the product design phase. That is how this technology/service can serve to preserve those fundamental rights, rather than at the last stage, i.e. the implementation phase.

Ethics by design, safety by design, and privacy by design should be looked at more closely, and play a bigger role in future regulation. Companies should be expected to incorporate these principles into their product development cycles at an early stage and be accountable to those principles. There are already some positive examples of compliance with design obligations around safety by design, and privacy by design mentioned in the GDPR. Adding safety by design and privacy by design as part of the initial product development cycle makes it extraordinarily difficult to abuse a platform. Some large companies also consider such principles as a pre-condition for third party partnership.

The overarching question remains whether personal data form part of the business model of the company in question, and whether that data are monetised by (small and large) online platforms. It is worth looking beyond online platforms, to the wider commercial ecosystem that enables and rewards the dissemination and amplification of harmful content on the platform, and shares a common understanding of the business models operating in the background, in particular around ad tech. From what source does the content originate? How is it being disseminated and amplified? What are the economic incentives upon which to decide the need for intervention? Unless we understand the incentives and understand the business models, regulatory bodies will be playing catch up.

Looking at the business models potentially requires engaging with several different regulatory regimes, not only around platform liability, but also data protection, and competition. It will be important that all the regulatory bodies upon which the regime are based are engaged in the discussion on the design of the principles.

While this topic may be very complex, it should not remain deliberately opaque. More educational efforts would be welcome to avoid misconception and wrong assumptions by regulators and industry players on how online platforms work and to understand why it is rewarding for some third party players (individuals, companies, states) to disseminate fake news and illegal content on online platforms.

Should **stricter responsibility** be imposed according to the **type** of illegal and/or harmful **content**?

RESPONSES

Certain types of illegal content represent a real danger to public safety. Public safety should be paramount to all stakeholders and regulators and require, therefore, a stricter responsibility to remove dangerous online content, such as terrorist materials, more quickly. A majority of platforms are already taking such materials down within an hour upon notice. Such conduct has become a de facto standard. Regarding other illegal content, 24 hours is the usual standard used by online platforms. Although this standard is not mandatory, it has now become a de facto standard for most online platforms. The shared objective of public safety will repeatedly have to be prioritised.

Should **stricter responsibility** be imposed according to the **size of the online platform**? Should a new legal category of *Public Space Content Sharing Platforms* be created to impose such additional responsibility?

RESPONSES

Online platforms that, by their nature (user base, functionality, reach, role), pose a greater risk should be subject to more obligations than lower risk ones. Hence, asymmetry based on the risk of harm instead of the size of the platform is seen as a good approach. However, the principle of proportionality, as opposed to the principle of symmetry, should be considered here as more future-proofed.

Improving platforms oversight and rules enforcement

Should oversight and enforcement be differentiated according to the size of the platform?

Should there be an EU level enforcement body or enhanced collaboration among national regulatory authorities? (For example, should the largest platforms be regulated by an EU body while the other platforms continue to be regulated by the authority of the member state where they are established as it is the case for the financial supervision of European banks)?

RESPONSES

Effective enforcement and supervision are essential. GDPR is a great example of a set of rules that is pretty robust, principled-based, and works horizontally across sectors, but has limited success when it comes to enforcement and supervision of its implementation across the Member States. Although it is complex for national regulatory bodies to enforce regulation on large platforms, the idea of the European Single Market and a single European regulatory body should not be overlooked. Another alternative could be for issues affecting more than three member states to be elevated to the European level.

Should there be a Regulation imposed across the EU, a means for ensuring the cost of compliance with that Regulation is not too high for smaller players would be needed, and avoid creating an additional barrier to competition and innovation. There needs to be flexibility in the way that the firms design their compliance programs.

Content-related rules usually reflect national sensitivities and prevent anyone else except the local regular authority from intervening. There is consensus around the idea that most illegal or dangerous content in most of the member states is generally speaking illegal for all Member States, and that cultural exceptionalism is often used for protectionist reasons.

Should we continue to rely on **Codes of Conduct** for a safer Internet? How could existing Codes of Conduct be improved at the establishment and monitoring stages, and in what other areas might codes be needed, if any?

RESPONSES

A less static but more collaborative approach based on ongoing dialogues between regulators and online platforms can be very useful to achieve the main regulatory goals. One difficulty will be working with platforms from different continents (mainly America or China), that sometimes subscribe to different values and could make collaboration with European regulatory authorities even more complicated.

Over the last few years, Codes of Conduct have shown some positive effects in key areas of illegal content such as hate speech. More platforms should also be encouraged to sign Code of Conducts that would ideally be short and principle-based to supplement the baseline rules. The Codes should also have clear objectives, and their implementation should involve regular independent and transparent monitoring, as well as effective and proportionate sanctions.



RECOMMENDATIONS PAPER

RECOMMENDATIONS PAPER

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.¹⁰⁰ The European Parliament adopted three resolutions which have been prepared by the IMCO, the JURI and the LIBE Committees.¹⁰¹ 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.¹⁰² 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.¹⁰³ 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.

¹⁰⁰ Communication from the Commission of 19 February 2020, Shaping Europe's digital future, COM(2020) 67.

¹⁰¹ https://www.europarl.europa.eu/doceo/document/TA-9-2020-10-20-TOC_EN.html

¹⁰² 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>

¹⁰³ 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

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.¹⁰⁴ 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.¹⁰⁵ 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,¹⁰⁶ and requires those not established in the EU to designate a representative in the EU.¹⁰⁷ **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.**¹⁰⁸

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.¹⁰⁹ 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

¹⁰⁴ 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)

¹⁰⁵ 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).

¹⁰⁶ 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.

¹⁰⁷ GDPR, art.27.

¹⁰⁸ See AVMSD, art. 2(5, 5a, 5b & 5c)

¹⁰⁹ AVMSD, art.3(2).

for derogation given the substantial strengthening of the EU consumer acquis since the enactment of the ECD.¹¹⁰

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.

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 procedures¹¹¹ or functionalities afforded to users that allow them to take responsibility for exposure to legal content¹¹². 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.

¹¹⁰ 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.

¹¹¹ Such as those in Art. 28(b)(3) lines d, e, and i that cover systems for flagging and reporting content and handling complaints.

¹¹² such as those in Art. 28(b)(3) lines f, g and h that cover age verification, content rating and parental controls.

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 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.¹¹³ 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.¹¹⁴ 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

¹¹³ 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.

¹¹⁴ 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.

demonstrably fail to meet their obligations, which would be dealt with by the courts, under the coordination of the Court of Justice jurisprudence.

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.¹¹⁵ 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.¹¹⁶ 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.¹¹⁷ The following is a 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.

¹¹⁵ 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>

¹¹⁶ 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:.

¹¹⁷ 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;
- Expedient 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.¹¹⁸

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.

¹¹⁸ These might include civil society and human rights organisations investigating incidents of war crimes or abuses and not solely national law 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.¹¹⁹ 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.¹²⁰

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.¹²¹

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 European Regulators Group for Audiovisual (ERGA), the creation and then the reinforcement of the Consumer Protection Cooperation (CPC) Network¹²² and the increasing use of the Internal Market

¹¹⁹ See AVMSD, new Article 4a introduced by Directive 2018/1808.

¹²⁰ 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.

¹²¹ 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.

¹²² 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.



Information (IMI) System.¹²³ **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.

¹²³ 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.

ABOUT CERRE

Providing top-quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.



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)