



# Unravelling the Digital Services Act package

**IRIS *Special***

A publication  
of the European Audiovisual Observatory



IRIS *Special* 2021-1

**Unravelling the Digital Services Act package**

European Audiovisual Observatory, Strasbourg 2021

**Director of publication** – Susanne Nikoltchev, Executive Director

**Editorial supervision** – Maja Cappello, Head of Department for legal information

**Editorial team** – Francisco Javier Cabrera Blázquez, Léa Chochon, Sophie Valais, Legal Analysts  
European Audiovisual Observatory

**Authors** (in alphabetical order)

Joan Barata, Oliver Budzinski, Mark Cole, Michèle Ledger, Tarlach McGonagle, Katie Pentney, Eleonora Rosati, Alexandre de Stree

**Translation**

Julie Mamou, Nathalie Sturlèse, Stefan Pooth, Erwin Rohwer

**Proofreading**

Anthony Mills, Catherine Koleda, Gianna Iacino

**Editorial assistant** – Sabine Bouajaja

**Press and Public Relations** – Alison Hindhaugh, [alison.hindhaugh@coe.int](mailto:alison.hindhaugh@coe.int)  
European Audiovisual Observatory

**Publisher**

European Audiovisual Observatory

76, allée de la Robertsau

F-67000 Strasbourg, France

Tél. : +33 (0)3 90 21 60 00

Fax : +33 (0)3 90 21 60 19

[iris.obs@coe.int](mailto:iris.obs@coe.int)

[www.obs.coe.int](http://www.obs.coe.int)

**Cover layout** – ALTRAN, France

**Please quote this publication as:**

Cappello M. (ed.), *Unravelling the Digital Services Act package*, IRIS *Special*, European Audiovisual Observatory, Strasbourg, 2021

© European Audiovisual Observatory (Council of Europe), Strasbourg, October 2021

Opinions expressed in this publication are personal and do not necessarily represent the views of the European Audiovisual Observatory, its members or the Council of Europe

# Unravelling the Digital Services Act package

Joan Barata, Oliver Budzinski, Mark Cole, Alexandre de Stree, Michèle Ledger,  
Tarlach McGonagle, Katie Pentney, Eleonora Rosati





# Foreword

In 2019, the European Commission launched the process for the adoption of the so-called Digital Services Act package, which aims at modernising the current legal framework for online intermediary services. As a result of this process, two new Regulation proposals, the Digital Services Act (DSA) and the Digital Markets Act (DMA) were published on 15 December 2020.

At a key point in the discussions on this new legislative framework, the European Audiovisual Observatory organised a series of webinars dealing with specific topics, where the areas of interplay between the Digital Services Act package and existing regulatory instruments may appear more complex. The aim was to help pave the way for a structured exchange among academic experts and stakeholders, with the participation of European Commission representatives to help set the scene and the Observatory team acting as facilitator for the exchange. An initial introductory conference offering a first look at the new EU rules on online services and their possible impact on the audiovisual industry took place on 11 February 2021, and four webinars dealing, respectively, with content moderation, gatekeepers and VoD, copyright, and the fight against disinformation, took place between March and July 2021. All these events are available for viewing on the website of the Observatory at [www.obs.coe.int](http://www.obs.coe.int).

In parallel to these events, the Observatory invited the participating experts to contribute to the present publication, which aims at complementing and expanding what was said during the discussion. The report is divided in two main areas: one focusing on the DSA and the other on the DMA, each of them divided into two parts.

With regard to the DSA, the first part concerns the regulation of freedom of expression: in three consecutive chapters, Joan Barata, Alexandre de Stree/Michèle Ledger and Katie Pentney/Tarlach McGonagle discuss the intricacies of regulating speech in the online realm and the role that the DSA may play in this regard. The second part concerns copyright: Elenora Rosati provides a detailed presentation of the interplay between EU copyright rules and the DSA.

Concerning the DMA, the first part, written by Mark D. Cole, provides an overview of how this system will play out and interplay with other regulatory instruments. In the second part, Oliver Budzinski focuses on the economics of gatekeeping in the audiovisual sector and provides his insights about problems and possible solutions.

All these parts are prefaced by introductory texts written in-house. This publication also includes a short overview of the Digital Services Act package and, as an annex, a summary of the discussions that took place at the five Observatory events involving stakeholders from various audiovisual industry groups.

Working on this publication has been extremely rewarding and I would like to thank both the experts and the participants of the various DSA events who shared their experience (in alphabetical order): Joan Barata (Stanford Law School), Richard Burnley (EBU), Oliver Budzinski (Ilmenau University of technology), Paolo Celot (EAVI), Mark D. Cole (University of Luxembourg/European Institute for Media Law), Celene Craig (BAI), Alexandre de Stree

(University of Namur/CERRE), Cécile Despringre (SAA), Pauline Durand-Vialle (FERA), Siada El Ramly (Dot Europe), Miriam Estrin (Google), Marco Giorello (European Commission), Paula Gori (EDMO), Anna Herold (European Commission), Miruna Herovanu (ACT), Marisa Jiménez Martín (Facebook), Ľuboš Kukliš (ERGA), Alexandra Lebret (EPC), Stéphanie Martin (SAA), Stan McCoy (MPA), Tarlach McGonagle (University of Amsterdam), Maria Michalis (Euralva), Paige Morrow (Office of the UN Special Rapporteur on Freedom of Expression), Marco Pancini (YouTube), Greg Polad (ACT), Marc Putman (EUROVOD), Elenora Rosati (University of Stockholm), Anna Solar-Bassett (Vodafone), Martin Senftleben (University of Amsterdam), Krisztina Stump (European Commission), Charlotte Willner (Trust & Safety Professional Association).

Have a thought-provoking read!

Strasbourg, October 2021

**Maja Cappello**

IRIS Coordinator

Head of the Department for Legal Information

European Audiovisual Observatory

# Table of contents

---

<b>1. General introduction.....</b>	<b>1</b>
<b>2. The Digital Services Act and social media power to regulate speech: obligations, liabilities and safeguards .....</b>	<b>5</b>
2.1. Introduction .....	5
2.2. Public and private speech regulation.....	6
2.3. Intermediary Liability: From the E-Commerce Directive to the DSA .....	8
2.4. Liability regimes under the DSA.....	11
2.4.1. Introduction .....	11
2.4.2. Notice-and-action mechanisms.....	11
2.4.3. Own-initiative investigations.....	12
2.4.4. Interpretation issues around Article 6 DSA.....	13
2.5. Assessment and mitigation of systemic risks.....	15
2.5.1. Assessment of systemic risks.....	15
2.5.2. Mitigation of systemic risks .....	18
2.6. Conclusions.....	19
<b>3. Regulating the moderation of illegal online content.....</b>	<b>20</b>
3.1. Scope and structure of this chapter .....	20
3.2. The independence of cyberspace: the e-Commerce Directive.....	21
3.3. The beginning of the end: The emerging EU regulatory framework for online content moderation	24
3.3.1. Regulation of the moderation of specific types of online content.....	24
3.3.2. Regulation of moderation by specific types of digital intermediaries: Video-sharing platforms.....	28
3.3.3. Regulation for all: A re-interpretation of the e-Commerce Directive.....	29
3.3.4. Summary of the EU regulatory framework and current practices of online moderation .	30
3.4. The end of the independence of cyberspace: The Digital Services Act.....	31
3.4.1. The proposed DSA and content moderation.....	32
3.4.2. Asymmetric obligations.....	33
3.5. Concluding remarks .....	36
<b>4. From risk to reward? The DSA's risk-based approach to disinformation... </b>	<b>40</b>
4.1. Introduction .....	40

4.2. The disinformation landscape.....	41
4.2.1. Evolving definitions .....	41
4.2.2. Broader regulatory and policy frameworks.....	44
4.3. Introducing the DSA's risk-based approach .....	47
4.4. Mitigating risks .....	50
4.5. Ensuring oversight and transparency.....	52
4.6. Risky business? The risk-based approach in action .....	54
4.7. Conclusion.....	56

---

## **5. The Digital Services Act and copyright enforcement: The case of Article 17 of the DSM Directive\* ..... 59**

5.1. Introduction .....	59
5.1.1. The shared history of the DSM Directive and the DSA .....	60
5.2. Structure and content of Article 17 of the DSM Directive .....	64
5.2.1. Polish challenge to Article 17 .....	66
5.3. The relationship between Article 17 and the DSA: What is special about it? .....	67
5.3.1. Notion of OCSSP: EU establishment, accessibility, and targeting .....	67
5.3.2. The specific liability mechanism of Article 17(4).....	69
5.3.3. Safe harbour availability .....	72
5.3.4. The complaint and redress mechanism and protection against misuse .....	73
5.4. Conclusion.....	74

---

## **6. The proposal for a Digital Markets Act (DMA): On gatekeepers, fairness and transparency in the online environment ..... 76**

6.1. Introduction .....	76
6.2. The DMA in a nutshell.....	78
6.3. Scope of Application: Broad but few .....	81
6.3.1. Actors addressed.....	81
6.3.2. Designation procedure.....	85
6.4. Obligations and Prohibitions or 'Do's and don'ts' for Gatekeepers .....	86
6.4.1. Structural aspects.....	86
6.4.2. Close-up on some of the obligations .....	88
6.5. Enforcement: A centralised approach.....	90
6.6. Conclusion.....	92

---

## **7. Gatekeeping in the audiovisual sector: economic background, competition, and regulation ..... 94**

7.1. Introduction .....	94
7.2. Competition and gatekeepers in the digital economy: The underlying economics.....	96
7.3. Competition and gatekeeping in streaming markets .....	102
7.4. Regulatory implications for audiovisual streaming markets from an economic perspective.....	105
7.4.1. Self-Preferencing .....	105
7.4.2. Vertical Integration .....	107
7.4.3. Summary .....	108

---

## **8. Summaries of the series of EAO events on the DSA Package .....110**

8.1. A first look at the new EU rules on online services and their possible impact on the audiovisual industry.....	110
8.1.1. Setting the scene: Overview of the new Digital Services Act Package.....	110
8.1.2. The experts' corner: Competition, liability and interaction between the DSA Package, the AVMS Directive and the DSM Directive .....	111
8.1.3. The stakeholders' panel: The DSA, a much-needed update of an outdated legal framework.....	112
8.2. Webinar #1 - Transparency of content moderation on social media.....	113
8.2.1. Setting the scene .....	113
8.2.2. The expert's corner: Online platforms' moderation of illegal content online.....	114
8.2.3. The stakeholders' panel: Content moderation from the perspective of platforms, consumers and media NRAs .....	115
8.3. Webinar #2 - Gatekeepers in the DSA Package: What about VoD? .....	116
8.3.1. Setting the scene .....	116
8.3.2. The expert's corner: Regulatory and competition-related aspects .....	117
8.3.3. The stakeholders' panel: The VoD market, a competitive and heavy regulated market without gatekeepers?.....	117
8.4. Webinar #3 - Copyright and the digital services act.....	119
8.4.1. Setting the scene .....	119
8.4.2. The experts' corner: Risks and opportunities of the DSA .....	120
8.4.3. The stakeholders' panel: Interplay between the DSA and copyright, risks, challenges, and opportunities .....	120
8.5. Webinar #4 - The Digital Services Act and the fight against disinformation.....	122
8.5.1. Setting the scene .....	122
8.5.2. The expert's corner: Risks and opportunities for the fight against disinformation.....	122
8.5.3. The stakeholders' panel: Tackling disinformation, freedom of expression and access to data .....	123
8.6. List of participants.....	125

## Figures

Figure 1.	DSA obligations .....	2
Figure 2.	Working definitions of disinformation.....	43

## Tables

Table 1.	EU regulatory framework on moderation of illegal content online.....	30
----------	--	----

# 1. General introduction

Everyone has seen funny videos of cats on the Internet, but this is a rather recent development. I am sure that most of you still remember the good old times when you could not share YouTube videos of kitties with your Facebook friends, or tweet about them with just a click on your smartphone.

Those services are regulated at the European level by a rather old legal instrument: the so-called Directive on electronic commerce, also known as the e-commerce Directive.

One advantage of the rules contained in this directive is their simplicity. They are straightforward, everything is clear. They also have clear effects. Like a modern Pontius Pilate, service providers can virtually wash their hands of whatever users do. In theory, at least. So what is the problem with this directive? Well, for starters, this directive is a regulatory answer to problems apparent in the year 2000. A world without Facebook, YouTube and iPhones. And very importantly, despite its given name, the e-commerce Directive regulates much more than just commerce, because these services have an impact on freedom of expression, on cultural diversity, on copyrighted works, even on free elections. Now, the question is whether this simple, straightforward legal solution is fit for purpose in 2021, that is, in a world that has become way more complicated. Of course, the beauty of the e-commerce Directive lies in its simplicity. Adding layers of regulation increases complexity which could lead to confusion, overlapping, and even contradiction between different legal norms. Moreover, the fundamental nature of freedom of expression limits the legislator's room for manoeuvre.

In Europe, change has been in the making for quite a long time. The European Union has already introduced exceptions to the e-commerce Directive rules a.o. in two legal instruments:<sup>1</sup>

- The 2018 revision of the Audiovisual Media Services Directive (AVMSD) extended the directive's scope to cover video-sharing platforms (VSPs).
- Article 17 of the Directive on Copyright in the Single Market (DSM) introduced new obligations for online content sharing platforms (OCSPs).

In 2019, the European Commission launched the process for the adoption of a more comprehensive regulatory package, the so-called Digital Services Act package (DSA). As a result of this process, two new Regulation proposals, the Digital Services Act and the Digital Markets Act, were published on 15 December 2020.

The Digital Services Act is a bit like a Russian doll. It provides rules for Intermediary services offering network infrastructure, with special rules for hosting services, online

---

<sup>1</sup> For a full picture of the regulation of online services as it stands today see Chapters 2 and 3 of this publication.

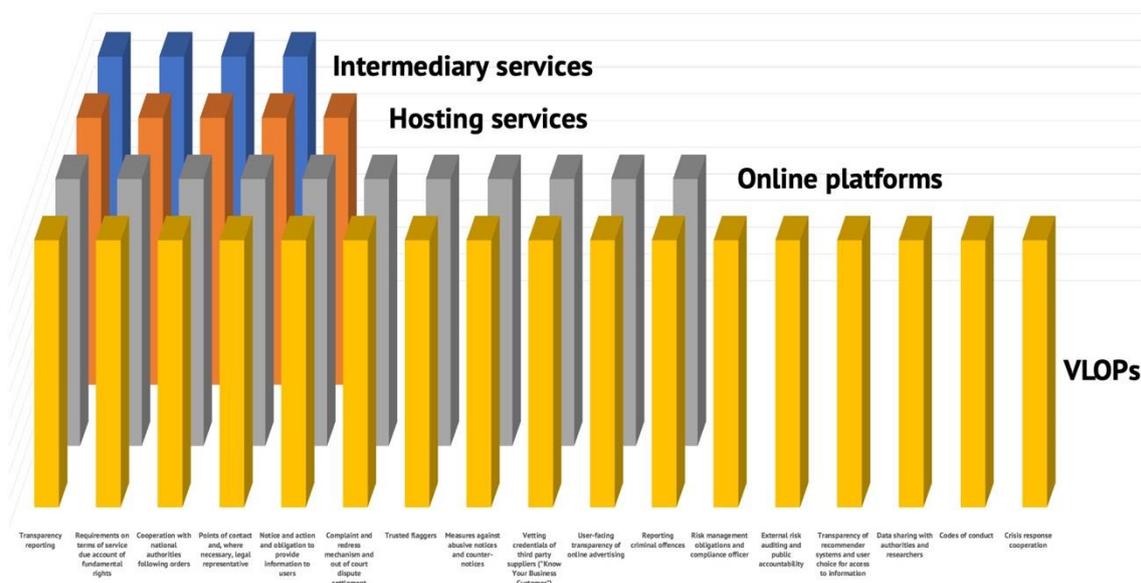
platforms and very large platforms. Very large platforms are online platforms that reach more than 10% of the EU's population (45 million users) and are considered systemic in nature.

The DSA will introduce a series of obligations graduated on the basis of the size of the service and impact, such as:

- measures to counter illegal goods, services or content online;
- new obligations on traceability of business users in online marketplaces;
- effective safeguards for users;
- transparency measures for online platforms;
- specific obligations for very large platforms to prevent the misuse of their systems;
- access for researchers to key data of the largest platforms, to allow understanding of how online risks evolve;
- oversight structure to address the complexity of the online space.

As depicted in the following graph, intermediary services are subject to some basic obligations, to which further obligations are added, depending on the nature and size of the service.

**Figure 1. DSA obligations**



Source: OBS

If the DSA rules look like a Russian doll, the Digital Markets Act (DMA) looks more like Hercules trying to capture Cerberus. As you surely know, Cerberus was in Greek and Roman mythology the gatekeeper of Hell.

The DMA regulates gatekeepers of a slightly different place: the Internet. Gatekeepers are those online platforms that have a significant impact on the Internal



Market, serve as an important gateway for business users to reach their customers, and which enjoy, or will foreseeably enjoy, an entrenched and durable position.

In a nutshell, the Digital Markets Act will:

- define quantitative thresholds as a basis to identify presumed gatekeepers. The European Commission will also have powers to designate companies as gatekeepers following a market investigation;
- prohibit a number of practices which are clearly unfair;
- require gatekeepers to proactively put in place certain measures;
- impose sanctions for non-compliance to ensure the effectiveness of the new rules;
- allow the European Commission to carry out targeted market investigations.

As was to be expected, the publication of these two Regulation proposals has raised hopes, fears and, most of all, questions – lots of questions.

The scope of both the DMA and DSA includes video-sharing platforms such as YouTube and the like but excludes video-on-demand platforms such as Netflix, Amazon Prime or Disney+. VoD providers remain subject to the obligations of the audiovisual media services directive, as they imply editorial responsibility, an element lacking in the case of intermediaries, to which the DSA applies.

It is too early to say how this system will look in practice, as the co-decision procedure is still ongoing among EU institutions. In the meantime, reading the following chapters of this publication will give you plenty to think about.



## **Regulating the speech of others**

*The idea of regulating speech may be alien to many citizens of democratic countries: isn't speech by nature free? Obviously, it is not that simple. Like any other freedom, speech carries with it duties and responsibilities, and therefore may be subject to legal restrictions. The question is: who is in charge of imposing and policing such restrictions?*

*Let's not forget that legislating is, or should be at least, the delicate art of balancing interests. Freedom to conduct business, on one side of the balance, and consumer protection, on the other. Freedom of expression, on one side, and protection of other rights, on the other. It is a delicate and complex art.*

*Legislating is also the art of defining. And defining is also complex. Because to define, as Oscar Wilde wrote, is to limit. The most important definitions in law concern the difference between "legal" and "illegal". Whatever is not illegal is legal, isn't it? Well, it is never that simple, as mentioned before. Even less simple is the difference between "illegal" and "harmful". There is a general agreement among stakeholders that "harmful" (yet not, or at least not necessarily, illegal) content should not be defined in the Digital Services Act and should not be subject to removal obligations, as this is a delicate area with severe implications for the protection of freedom of expression.*

*Because, what is harmful? As long as it is not defined by the law, it is subjective. There is plenty of offensive content on the Internet, you may say. But offensive to whom? And why should offensive content be removed? And most importantly, who decides about these questions if not the law or a judge?*

*Social media has taken on this job to a great extent.*

*Social media providers will tell you that content moderation is like the fable of the miller, the son and the donkey: whatever they do, remove, not remove, they will be criticised. But if we put aside the most notorious cases, it is true that content moderation is a sort of Mission Impossible, given the amount of data to be sifted through and the resources required. Artificial intelligence is presented as part of the solution for this problem, but its lack of "humanity" is precisely one of its biggest drawbacks. Filtering algorithms are extremely efficient in addressing and removing potential harmful content, but they cannot match humans in making nuanced decisions on complex legal areas.*

*In three consecutive chapters, **Joan Barata, Alexandre de Stree/Michèle Ledger and Katie Pentney/Tarlach McGonagle** discuss the intricacies of regulating speech in the online realm and the role that the DSA may play in this regard.*

## 2. The Digital Services Act and social media power to regulate speech: obligations, liabilities and safeguards<sup>2</sup>

*Joan Barata, Intermediary Liability Fellow, Program on Platform Regulation, Cyber Policy Center, Stanford University*

### 2.1. Introduction

In mid-December 2020, EU Commissioners Margrethe Vestager and Thierry Breton presented two major legislative proposals<sup>3</sup> aimed at defining a new regulatory regime applicable to Internet intermediaries. The proposals in question are the Digital Services Act (DSA) and the Digital Markets Act (DMA).

The DMA is in particular aimed at harmonising existing rules in member states, in order to better prevent the formation of bottlenecks and the imposition of entry barriers to the digital single market. The DSA establishes a series of fundamental rules and principles regarding, essentially, the way intermediaries participate in the publication and distribution of online content. It especially focuses on content hosting and sharing platforms, such as Facebook, TikTok, Twitter, and YouTube.

This article will focus on a series of specific aspects of the DSA proposal.<sup>4</sup>

The analysis will firstly aim at identifying to what extent the new draft encourages the adoption by intermediaries of initiatives aimed at dealing with illegal and other forms of objectionable content, either on the basis of their own investigations or as the result of third-party notices. In particular, it will focus on the interplay between lack of knowledge/awareness as a pre-condition to enjoy liability exemptions and the special protections granted to platforms when engaging in the initiatives mentioned above. In addition, it is also necessary to analyse how in particular the new regime overlaps and interacts with the so far jurisprudential approach based on the “neutrality” of the service provided by the platform.

---

<sup>2</sup> This article is based on a piece published by the author in the Verfassungsblog and titled “The Digital Services Act and the Reproduction of Old Confusions”, <https://verfassungsblog.de/dsa-confusions/>, and the text of the report “The Digital Services Act and its impact on the right to freedom of expression: special focus on risk mitigation obligations” (<https://libertadinformacion.cc/wp-content/uploads/2021/06/DSA-AND-ITS-IMPACT-ON-FREEDOM-OF-EXPRESSION-JOAN-BARATA-PDLI.pdf>).

<sup>3</sup> <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>.

<sup>4</sup> <https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN>.

Secondly, it will also focus on a specific type of “protected” content moderation practices: those enshrined and applicable to very large online platforms (VLOPs) according to Articles 26 and 27 regarding the mitigation of so-called systemic risks.

## 2.2. Public and private speech regulation

States have the power to define, within the framework of applicable international and regional standards, the legitimate limits and conditions to the exercise of the right to freedom of expression, thus differentiating between legal and illegal content.

Besides this, hosting providers generally moderate content according to their own – private – rules. Content moderation consists of a series of governance mechanisms that structure participation in a community to facilitate cooperation and prevent abuse. Platforms tend to promote the civility of debates and interactions to facilitate communication among users by setting and enforcing private content rules. Platforms also have the power to shape and regulate online speech beyond legal and statutory content provisions. Platforms’ content policies are often based on a complex mix of different principles: stimulating user engagement, respecting certain public interest values (genuinely embraced by platforms or as the result of policymaker and legislator pressure), or adhering to a given notion of the right to freedom of expression.

Platforms also play a fundamental role in determining what content is visible online and what content – although published – remains hidden or less prominent. Despite the fact that users are free to directly choose content delivered via online hosting providers (access to other users’ profiles and pages, search tools, embedding...), platforms’ own recommender systems are extremely influential inasmuch as they are in a central position among their interfaces and have become key content discovery features.<sup>5</sup> Given that final recommendation results are the outcome of a bilateral interaction between the user – including their preferences, bias, background, etc. – and the recommender systems themselves, it also needs to be underscored that the latter play an important gatekeeping role in terms of prioritisation, amplification or restriction of content.

Many authors and organisations have warned that intermediaries promote content in order to maximise user engagement, addiction, behavioural targeting, and polarisation.<sup>6</sup> On the other hand, it is also important to note that public understanding of platforms’ content removal operations, even among specialised researchers, has long been limited, and this information vacuum leaves policymakers poorly equipped to respond to concerns about platforms, online speech, and democracy. Recent improvements in company disclosures may have mitigated this problem, yet a lot is still to be achieved.<sup>7</sup> This being

---

<sup>5</sup> See a recent and thorough analysis on these matters in Leerssen P., “The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems”, *European Journal of Law and Technology*, 11(2),2020.

<sup>6</sup> Bietti E., “Free Speech is Circular”, *Medium*, 2020, <https://medium.com/berkman-klein-center/free-speech-is-circular-trump-twitter-and-the-public-interest-5277ba173db3>.

<sup>7</sup> Keller D. and Leerssen P., “Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation”, in Persily N. & Tucker J., *Social Media and Democracy: The State of the Field and Prospects for Reform*, Cambridge University Press, 2020.



said, it is also worth noting that big platforms already have a long record of mistaken or harmful moderation decisions in areas such as terrorist or extremist content.<sup>8</sup>

In the sphere of online platforms, the first type of legislation which needs to be considered establishes rules and sanctions directly aimed at platform users, specifying what they may or may not do, with what legal effect, and what the sanctions are. These rules and sanctions can be general (as is the case for hate speech, which uses to be defined in criminal codes) or specific (some states criminalise in particular the dissemination of terrorist content via online platforms, for example, due to its alleged wide reach.) Legislation of online speech is also integrated via legal rules meant to induce providers of digital services to influence the activity of their users: intermediaries are the direct target of the regulation, but the ultimate objective involves the users. Last but not least, legislation and regulation of online speech incorporate rules that are meant to regulate the activity of regulators when monitoring or regulating the activities of intermediary service providers, in cases where the latter “regulate” or moderate the activities of users.<sup>9</sup>

The first type of legislation and regulation clearly constitutes a potential interference with the right to freedom of expression. It speaks to basically “content rules” which are applied within the context of a bilateral relationship between the speaker and the state authorities. Therefore, usual safeguards and restrictions applicable to the regulation of the right to freedom of expression must apply to this kind of rules.

The following two categories (regulation of platforms’ activities and decisions, and definition of the role of regulators vis-à-vis online intermediaries) also have implications and impact the exercise of the right to freedom of expression, although they probably need to be seen as modalities of what can be called indirect state action. These rules are very much present in several pieces of legislation already adopted by EU institutions, and they have been incorporated into the proposal of the DSA, as will be further analysed below.

---

<sup>8</sup> See York J.C. and Gullo K., “Offline/Online Project Highlights How the Oppression Marginalized Communities Face in the Real World Follows Them Online”, *Electronic Frontier Foundation*, 2018, <https://www.eff.org/deeplinks/2018/03/offlineonline-project-highlights-how-oppression-marginalized-communities-face-real>; Perrigo B., “These Tech Companies Managed to Eradicate ISIS Content. But They’re Also Erasing Crucial Evidence of War Crimes”, *Time*, 2020, <https://time.com/5798001/facebook-youtube-algorithms-extremism/?xid=tcoshare>; “When Content Moderation Hurts”, *Mozilla*, 2020, <https://foundation.mozilla.org/en/blog/when-content-moderation-hurts/>.

<sup>9</sup> This classification is taken from Sartor, G. and Loreggia A., “The impact of algorithms for online content filtering or moderation European Parliament’s Directorate-General for Internal Policies, Policy Department for Citizens’ Rights and Constitutional Affairs, 2020, [https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL\\_STU\(2020\)657101](https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)657101).



## 2.3. Intermediary Liability: From the E-Commerce Directive to the DSA

The DSA (which will officially adopt the form of a Regulation) will complement the E-Commerce Directive<sup>10</sup> and introduce a series of new provisions applicable to online intermediaries. These provisions are of particular interest inasmuch as they impose on the mentioned providers several obligations particularly focused at limiting their “power” as well as better protecting the rights and interests of users.

The E-Commerce Directive contains, among other relevant aspects, the general intermediary liability regime applicable to intermediary service providers, notably hosting providers at the EU level. In order to retain liability exemption, platforms must not have actual knowledge of illegal activity or information and/or not be aware of facts or circumstances from which the illegal activity or information is apparent and upon obtaining such knowledge or awareness, must act expeditiously to remove or to disable access to the illegal content (Article 14 E-Commerce Directive).

The case law of the Court of Justice of the European Union (CJEU) has provided, under the E-Commerce regime, the criteria to determine where such knowledge and/or awareness exists. As established in the *L’Oréal* case,<sup>11</sup> rules set out in Article 14(1)(a) of the Directive “must be interpreted as covering every situation in which the provider concerned becomes aware, in one way or another, of such facts or circumstances”. The Court also limits liability to cases where the intermediary “plays an active role of such a kind as to give it knowledge of, or control” over the hosted content. In other words, intermediaries enjoy liability exemptions inasmuch as they perform a role of a mere technical, automatic, and passive nature. Despite the efforts of the Court in a very limited number of cases, it remains challenging to establish agreed criteria according to which intermediaries’ interventions can clearly be classified as active or passive (with the corresponding consequences in terms of liability).

National courts have also struggled with the distinction between active and passive intermediary services. After several contradictory decisions from lower courts, the Italian Supreme Court issued in 2019 a decision in the case of *Reti Televisive Italiane S.p.A v Yahoo!*<sup>12</sup> acknowledging and defining the mentioned distinction. According to the Court, intermediaries cannot benefit from “safe harbour” defences on the basis of Article 14 of the Directive in cases where, once again, the provider of information society services carries out an activity beyond a mere technical, automatic and passive service. In particular, the Court considers that hosting providers may be considered to play an active role in cases where they engage in activities such as filtering, selection, indexing, organisation, cataloguing, aggregation, evaluation, use, modification, extraction, or promotion of

---

<sup>10</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, <https://eur-lex.europa.eu/eli/dir/2000/31/oj>.

<sup>11</sup> Judgement of 12 July 2011, case C-324/09, <https://curia.europa.eu/juris/document/document.jsf?jsessionid=B972AF02024FAB1F627A43F6B09A7BB5?text=&docid=107261&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1122018>.

<sup>12</sup> Court of Cassation, First civil division, ruling no. 7708/2019, published March 19, 2019, [http://www.cortedicassazione.it/cassazione-resources/resources/cms/documents/7708\\_03\\_2019\\_no-index.pdf](http://www.cortedicassazione.it/cassazione-resources/resources/cms/documents/7708_03_2019_no-index.pdf).



content. In those cases, the intermediary may not benefit from liability exemptions provided by the E-Commerce Directive and may thus be subjected to the general liability regime established under civil law.<sup>13</sup>

Connected to Article 14, Article 15 prohibits the imposition of general content-monitoring obligations, as well as obligations “to (actively) seek facts or circumstances indicating illegal activity”. In the words of the CJEU in, once again, the *L’Oréal* decision, “the measures required of the online service provider concerned cannot consist in an active monitoring of all the data of each of its customers”, although it can be ordered to take specific measures in order to terminate a particular infringement and/or facilitate the identification of an individual offender. In *Scarlet Extended*<sup>14</sup> and *SABAM*<sup>15</sup> the Court specifically established that national courts are precluded from issuing injunctions against hosting service providers which require them to install a system for filtering, when such a system would actively monitor all the data of each of their customers in order to prevent future legal infringements.

It can thus be concluded that in the EU legal system intermediaries become liable, as a general principle, when they are proven to have overlooked a particular illegality when implementing voluntary measures in such a way as to create actual or constructive knowledge.

Another important conclusion regarding the complex interpretative parameters mentioned above is the fact that making the liability exemption conditional on a blurry definition of “passivity” induces a hands-off approach that may result both in an increased quantity of online illegalities and in the failure to satisfy the users who prefer not to be exposed to objectionable or irrelevant material.<sup>16</sup>

It is important to note that, in light of this jurisprudence, Articles 14 and 15 of the E-Commerce Directive would in principle need to be read and interpreted in a separate manner. While the former establishes knowledge and awareness thresholds and parameters in order for hosting intermediaries to keep their liability exemptions, the latter frames the possible imposition of specific and targeted content monitoring duties. In this second case, legal responsibilities may be demanded of intermediaries according to national legislation, only when such duties have not been properly fulfilled.

It also needs to be noted that some recently adopted sector-specific legislation at EU level seems to incorporate new obligations regarding the adoption of proactive measures. These proactive measures would however be compatible – or rather

---

<sup>13</sup> See Rosati E., “Italian Supreme Court clarifies availability of safe harbours, content of notice-and-takedown requests, and stay-down obligations”, *The IPKat*, 2019, <https://ipkitten.blogspot.com/2019/03/italian-supreme-court-clarifies.html>

<sup>14</sup> Judgment of 24 November 2011, case C-70/10, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1122459>.

<sup>15</sup> Judgment of 16 February 2012, case C-360/10, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1122533>.

<sup>16</sup> Sartor G., “Providers Liability: From the eCommerce Directive to the future”, in-depth analysis for the IMCO Committee commissioned by the Policy Department for economic and scientific policy, Directorate-General for Internal Policies, European Parliament, 2017, [https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL\\_IDA\(2017\)614179\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf)



complementary – vis-à-vis the mentioned prohibition regarding content-monitoring obligations. In other words, despite the general prohibition included in Article 15, it can be noted that sector-specific legislation is progressively establishing new proactive monitoring obligations for intermediaries.

In this sense, the so-called Copyright Directive<sup>17</sup> contains a series of obligations vis-à-vis so-called online content-sharing service providers (OCSSP), particularly to ensure the unavailability of certain copyright-protected works (Article 17). Recital 70 states that such steps “should be without prejudice to the application of exceptions or limitations to copyright, including, in particular, those which guarantee the freedom of expression of users”. The Audiovisual Media Services Directive<sup>18</sup> encompasses a series of duties of so-called video-sharing platforms (VSPs) concerning the prevention and moderation of content that constitutes hate speech and child pornography, affects children’s physical and mental development, violates obligations in the area of commercial communications, or can be considered as terrorist content. Besides this, national authorities (mainly independent media regulatory bodies) are given the responsibility of verifying that VSPs have adopted “appropriate measures” to properly deal with the types of content mentioned above (alongside other undesirable content). Under this scheme, overseen in the last instance by public regulatory bodies, platforms not only bear a duty to adopt a wide range of measures regarding the possible dissemination of illegal content by users, but they may also have the obligation to provide them with proper redress mechanisms with regards to possible restrictions to their rights derived from the mentioned measures.<sup>19</sup> In this context, platforms are broadly requested to consider “the rights and legitimate interests at stake, including those of the video-sharing platform providers and the users having created or uploaded the content as well as the general public interest” (Article 28b(3) AVMSD). The recently adopted Regulation of the European Parliament and of the Council on addressing the dissemination of terrorist content online (TERREG)<sup>20</sup> contains important obligations for hosting service

---

<sup>17</sup> Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.), <https://eur-lex.europa.eu/eli/dir/2019/790/oj>. It is important to note that the Government of Poland has requested of the CJEU precisely the annulment of some of the provisions included in the mentioned article claiming that “the imposition on online content-sharing service providers of the obligation to make best efforts to ensure the unavailability of specific works (...) and the imposition on online content-sharing service providers of the obligation to make best efforts to prevent the future uploads of protected works (...) make it necessary for the service providers – in order to avoid liability – to carry out prior automatic verification (...) and therefore make it necessary to introduce preventive control mechanisms. Such mechanisms undermine the essence of the right to freedom of expression and information and do not comply with the requirement that limitations imposed on that right be proportional and necessary.” *Republic of Poland v European Parliament and Council of the European Union* (Case C-401/19), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=216823&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1125063>.

<sup>18</sup> Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (codified version) (Text with EEA relevance), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02010L0013-20181218>.

<sup>19</sup> See Barata J., Regulating content moderation in Europe beyond the AVMSD, *LSE Blog*, 2020, <https://blogs.lse.ac.uk/mediase/2020/02/25/regulating-content-moderation-in-europe-beyond-the-avmsd/>.

<sup>20</sup> Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0784>.

providers in terms of illegal content removal and putting in place specific measures to address the dissemination of terrorist content online. The Regulation incorporates imprecise guidelines establishing that when adopting such measures providers need to take into account “the risks and level of exposure to terrorist content as well as the effects on the rights of third parties and the public interest to information” (recital 22). Designated “competent authorities” (sic) will “determine whether the measures are effective and proportionate”.

## 2.4. Liability regimes under the DSA

### 2.4.1. Introduction

The DSA does not repeal the basic provisions established under the E-Commerce Directive in this field. It in fact contains substantially identical provisions regarding hosting service providers in its Article 5, thus keeping the core of the current conditioned intermediary liability regime untouched. It is important to underscore, however, that due to the fact that the DSA will adopt the legal rank of a Regulation, such provisions will become directly applicable without the mediation of national legislation (as is the case for Directives).

This being said, it is also important to note that the DSA incorporates new legal and regulatory layers which may lead to even more challenging interpretation issues that in the last instance will probably need to be addressed by the Court in Luxembourg as well.

### 2.4.2. Notice-and-action mechanisms

Apart from the provisions included in afore-mentioned Article 5, Article 14 of the DSA establishes the requirements for notice-and-action mechanisms to be considered to give rise to such knowledge or awareness. Although the basis of the notice-and-action mechanism is the existence of a specific illegal content item, the DSA deliberately refrains from providing a substantive definition of what would be considered illegal in this context, and in general, the context of the overall Regulation. Article 2g) of the DSA refers to illegal content as “any information, which, in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law”. In other words, the DSA refers to already existing legal provisions from the corresponding sector-specific legislation, either at the national or the EU level.

Paragraph 2 of the article establishes that notices must contain “an explanation of the reasons why the individual or entity considers the information in question to be illegal content”. Connected to this, paragraph 3 affirms that notices that include, among other things, such an explanation “shall be considered to give rise to actual knowledge or awareness”. This being said, it is important to underscore that the mere fact that a user



argues that a certain piece of content is illegal must not necessarily create knowledge or awareness for the purposes of Article 5, unless the notified content reaches a certain threshold of obviousness of illegality. In a similar sense, recital 22 establishes that notices need to be “sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and where appropriate act against the allegedly illegal content”. In any case it is also clear that the DSA, similarly to the E-Commerce Directive, does not provide clear guidance or indications regarding how to identify such obviousness or to appreciate the existence of a reasonable identification of illegal content. It is important to underscore that any possible uncertainty or vagueness in this area may only promote the over-removal of content from the side of platforms.

Last but not least, it must also be noted that also according to recital 22 of the DSA, the removal or disabling of access “should be undertaken in the observance of the principle of freedom of expression”. This general provision is in line with the language of EU sector-specific legislation, which incorporates, as has already been noted, the duty of platforms and the oversight responsibility of relevant authorities to take into consideration the impact on freedom of expression of certain measures and decisions, together with other elements such as their effectiveness and the effect on of other rights. In any case, most of these legal indications are considerably vague regarding the criteria, parameters and safeguards that would need to be considered or incorporated by platforms when adopting and implementing the measures. Moreover, no specific and detailed mandates – neither procedural, nor substantive – regarding proper consideration and protection of human rights are provided to administrative or judicial authorities in charge of overseeing these aspects. Public intervention appears to be mainly oriented towards guaranteeing that illegal content is effectively addressed or eliminated.

### 2.4.3. Own-initiative investigations

According to Article 6 of the DSA proposal, intermediaries may not lose their liability protections “solely because they carry out voluntary own-initiative investigations or other activities aimed at detecting, identifying and removing, or disabling access to, illegal content, or take the necessary measures to comply with the requirements of Union law, including those set out in this Regulation”. This may be connected to the notion of the “Good Samaritan principle” as originally enshrined in U.S. legislation. This principle ensures that online intermediaries are not penalised for taking steps to restrict illegal or other forms of inappropriate content. This rule is usually presented as protective of the activities and interests of intermediaries: when intermediaries are granted immunity for the content they handle, the law is in fact incentivising the adoption and implementation of private policies regarding illegal and other types of content that is lawful but that may be offensive or undesirable in a given context. The principle finds one of its earliest and most acknowledged embodiments in Section 230(c) of the Communications Act of 1934 (as amended by the Telecommunications Act of 1996). Section 230 has played a fundamental role in the development of the Internet as we know it. Under the protections set by US law, intermediaries have the incentive to operate and expand their businesses under a



predictable legal regime, to moderate the content they share, and specifically to deal with certain forms of objectionable speech.<sup>21</sup>

Important clues regarding liability provisions under the DSA are also to be found in recital 22, according to which providers can acquire actual knowledge and awareness through “own-initiative investigations or notices submitted to it by individuals or entities in accordance with this Regulation in so far as those notices are sufficiently precise and adequately substantiated”.

Recital 25 reinforces and elaborates the principle that the mere fact that providers undertake investigative activities “does not lead to the unavailability of the exemptions from liability set out in this Regulation, provided those activities are carried out in good faith and in a diligent manner”. In order to be shielded from liability, these investigations must aim at “detecting, identifying and acting against illegal content” or at complying with “the requirements of Union law, including those set out in this Regulation as regards the implementation of their terms and conditions”. It is also important to note that this Recital – the last phrase – acknowledges the “residual” applicability of the previously mentioned active versus passive/neutral roles criterium, in particular to cases where the mentioned exemptions would not apply. In the same sense, recital 18 underscores the fact that liability exemptions should not apply “where, instead of confining itself to providing the services neutrally, by a merely technical and automatic processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information”. In other words, the DSA seems to suggest that when engaging in activities mentioned in Article 6 intermediaries do not automatically become “active” in terms of liability.

Therefore, without prejudice to the applicability of the general regime described in the previous section, the DSA has introduced some additional provisions that appear to encourage, to a certain extent, the adoption and implementation of content moderation policies by platforms and may also significantly affect liability adjudications. However, this will also bring relevant interpretation problems.

#### 2.4.4. Interpretation issues around Article 6 DSA

Firstly, own-initiative investigations remain protected by immunity shields when they “solely” aim at two main objectives: dealing with illegal content or complying with other obligations intermediaries may have according to the DSA itself and other relevant EU legislation.

When it comes to the notion of “illegal content”, recital 12 of the proposal establishes that such a notion must be defined broadly as it covers “information relating to illegal content, products, services and activities”. The concept should be understood to refer to information that “under the applicable law is either itself illegal (...) or that relates to

---

<sup>21</sup> Barata J., “Positive Intent Protections: Incorporating a Good Samaritan Principle in the EU Digital Services Act”, *CDT blog*, 2020, <https://cdt.org/insights/positive-intent-protections-incorporating-a-good-samaritan-principle-in-the-eu-digital-services-act/>.



activities that are illegal”. Therefore, the definition of the scope and substance of illegal content is not to be found in the text of the Regulation, but in sector-specific legislation, either at the national or the EU level. In any case, illegal content as a broad category may present very diverse typologies, including manifestly illegal and criminally penalised content (child pornography), illegal content as defined by other sources of national legislation (for example, advertising certain products), content which would only be firmly considered as illegal upon a judicial decision requested by an interested party (defamatory content), or content that depicts or represents illegal activities taking place in the physical world (which could not be necessarily considered as illegal, as such). In this area, it would be important that hosting providers are entitled to make their own good-faith assessment on the basis of the principles of legality, necessity and proportionality (which by the way are not clearly spelled out in the text). In addition to this, and in line with the “Good Samaritan” principle which appears to be anchored in Article 6, in cases where the mentioned assessment is dismissed by the competent authority, this must not eliminate *per se* providers’ liability exemptions.

Regarding “other” obligations, it is important to look in particular into the duty of very large platforms (over 45 million users) to “put in place reasonable, proportionate and effective mitigation measures, tailored to (...) specific systemic risks”, as established in Article 27 of the proposal in connection with Article 26. The latter broadly conceptualises the mentioned systemic risks as the dissemination of illegal content – (paragraph a) – and creating negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child – (paragraph b). A last-but-not-least systemic risk – (paragraph c) – would consist of the creation of negative or foreseeable effects on the protection of public health, minors, or civic discourse, or to electoral processes and public security via “intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service”. These provisions, as will be further developed below, have some problematic aspects including their extreme openness and vagueness. Besides this, and despite the reference to reasonableness and proportionality included in Article 27, it is also important to note that the specific nature and scope of the specific mitigation measures is left to the discretion of platforms and, in the last instance, to the decisions from still not clearly identified national regulatory bodies under the overall oversight of the European Commission.

Secondly, how should “solely” be interpreted in this context? This adverb appears to limit liability exemptions to cases where platforms have not undertaken any other activity, beyond the mentioned own-initiative investigations, which would indicate specific knowledge of a concrete piece of content. In other words, the DSA does not cover other possible actions or measures that may lead the competent authority to establish the existence of actual knowledge or awareness. Possible examples of these would be the case of the reception of an order to provide information under Article 9, or a not properly substantiated notice or report by a third party when it has led to the consideration of a specific piece of content or the adoption of concrete measures – demotion, communication with the original author, etc.

The DSA thus does not incorporate a proper Good Samaritan clause in terms of what has already been mentioned. In order to provide adequate results, a Good Samaritan clause



needs to be accurately crafted and avoid any possible counterincentive. In the current wording of the DSA, as is the case for the E-Commerce Directive, one can still conclude that the more platforms play an active role in monitoring the content they host, the more possible it becomes to find a potentially illegal piece of content which would at least require some cautious consideration. In this context, as presented above, the chances of platforms being proved to have overlooked a particular illegality, and therefore the risk of liability, grow significantly<sup>22</sup>. Article 6 could thus lead to more removals as it would be safer for the hosting providers engaging in proactive monitoring to remain cautious and remove more, rather than less, in avoidance of liability<sup>23</sup>.

## 2.5. Assessment and mitigation of systemic risks

### 2.5.1. Assessment of systemic risks

Very large online platforms (VLOPs) as defined by Article 25 of the DSA proposal, that is to say those which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, will need to assume under the DSA new duties assessment and mitigation of “systemic risks”, as has already been noted. The existence and nature of such risks is not clearly described or proven by the legislator. Recital 56 proclaims that platforms “can set the rules of the game, without effectively identifying and mitigating the risks and the societal and economic harm they can cause”. The risks outlined in Article 26 are very much connected or related to general societal risks (which would exist with or without the intermediation of online platforms). The extent to which, and the manner in which, these risks may be aggravated and how this aggravation can be realistically and properly assessed by platforms is something which is only vaguely presented in the proposal thus creating a high degree of uncertainty for platforms, as well as granting excessive discretion to relevant authorities.

Article 26 aims at defining such systemic risks by classifying them in three broad categories.

#### 2.5.1.1. Dissemination of illegal content through VLOP services

Illegal content as a broad category may present very diverse typologies, as has already been noted. These typologies may, in addition, present substantial differences between member states.

---

<sup>22</sup> Kuczerawy A., “The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?”, *KU Leuven CiTiC*, 2019, <https://www.law.kuleuven.be/citip/blog/the-eu-commission-on-voluntary-monitoring-good-samaritan-2-0-or-good-samaritan-0-5/>.

<sup>23</sup> Kuczerawy A., “The Good Samaritan that wasn’t: voluntary monitoring under the (draft) Digital Services Act”, *Verfassungblog*, 2021, <https://verfassungblog.de/good-samaritan-dsa/>.



Article 26 has a very special approach to illegal content: it does not use the term to refer to specific pieces of information that would require the adoption of targeted measures by platforms (as in the case of notice-and-action mechanisms, for example), but to describe illegal content not only as a broad category, but also as something that needs to be assessed by VLOPs in bulk. This provision does not clarify how this qualification is granted: in other words, whether it refers to content that has already been declared illegal by a relevant authority or at least has already been the object of specific measures under the provisions of the DSA, or rather points to the foreseeability that still-to-be-produced illegal information could end up being disseminated via the mentioned platforms.

The wording of the provision seems to combine both approaches and to establish that platforms may need to articulate content moderation policies particularly targeting users, accounts, pages, etc. which are proven to have become (or may foreseeably become) sources of illegal content. In addition to this, there are no indications regarding the introduction of possible – and binding – safeguards aimed at avoiding unnecessary and disproportionate impacts on the exercise of the right to freedom of expression by users and third parties (neither by platforms themselves nor oversight bodies).

The provision does not acknowledge the fact that the identification of illegal content is strongly dependent on different areas of not necessarily harmonised national legislation, which therefore creates important discrepancies between member states.

#### 2.5.1.2. “Any negative effects” on the exercise of fundamental rights

Alinea b) of paragraph 1 of Article 26 describes as a systemic risk “any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child”, as enshrined in the Charter of Fundamental Rights.

This systemic risk is presented in a very problematic way. The provision uses the language “any negative effects”, which is not appropriate in terms of human rights law. To mention just an example, reporting on matters of public interest may sometimes have a negative effect on the right to public and family life of certain public individuals, although this effect is in most cases overridden by the preeminent protections granted by the European Convention on Human Rights and the case law of the European Court of Human Rights with regard to the right to freedom of expression and freedom of information. In other words, the reference to “any violation” of fundamental rights is made on the basis of the consideration of such rights as completely separated realities, and without considering the very frequent need to articulate an interpretation that properly ponders the presence of different conflicting rights.

#### 2.5.1.3. Intentional manipulation of the service

Probably the most problematic provision regarding the description of systemic risks is the one regarding the “intentional manipulation of ... service, including by means of inauthentic use or automated exploitation of the service, with an actual or foreseeable negative effect



on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security”.

This provision has serious implications vis-à-vis the right to freedom of expression. The references to negative effects on public health, minors (which needs to be understood as something different from “rights of the child” in the previous alinea), civic discourse, electoral processes and public security together with the mention of incompatibility, beyond the law, with terms and conditions, clearly show that platforms may face the legal responsibility (overseen by public bodies) to restrict access to lawful content (and therefore protected under the freedom of expression clause) which can be considered “harmful” under the very vague criteria. These criteria are subjected to very open interpretations that are dependent on largely different political approaches and sensitivities within the European Union.

The Explanatory Memorandum of the DSA states that “‘harmful’ (yet not, or at least not necessarily, illegal) content should not be defined in the Digital Services Act and should not be subject to removal obligations, as this is a delicate area with severe implications for the protection of freedom of expression”. However, it is obvious that removal decisions are not the only ones with a strong impact on the right to freedom of expression. Other internal measures adopted by platforms to limit the impact of certain systemic risks (as explained in the following section) may also potentially affect this broad category of legal-but-harmful content. In this sense, it is important to differentiate between cases of “pure” content moderation, that is to say decisions taken by platforms on their own initiative and on the basis of their private terms of service (Article 2.p DSA) in fact defining content moderation as “the activities undertaken by providers of intermediary services aimed at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility and accessibility of that illegal content or that information, such as demotion, disabling of access to, or removal thereof, or the recipients’ ability to provide that information, such as the termination or suspension of a recipient’s account”, and measures adopted on the basis of the legal obligations imposed by Articles 26 and 27 of the DSA.

The complex interplay between legality and terms of service becomes particularly visible in paragraph 2 of Article 26, which states that when assessing the different systemic risks, platforms shall take into account “how their content moderation systems, recommender systems and systems for selecting and displaying advertisements influence any of the systemic risks referred to in paragraph 1, including the potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions”.

It is important to note that Article 26 does not properly define when a risk is too great to justify the adoption of mitigation measures. In other words, political, economic and social life incorporates per se many disfunctions and risks within the context of modern societies. These problems, including illegal behaviours, exist in parallel with or independently from online platforms. The key element here is to properly assess to what extent intermediaries generate extra risks or intensify existing ones to an “unacceptable” level. The next big question is whether platforms can be put in the position of conducting such complex analysis and deciding on the best tools to deal with those negative effects.



It is necessary to highlight the very strong human rights implications that these tasks entail. A particular element to be taken into account here is that Article 26 does not differentiate (nor establishes the need to differentiate) between different types of content when assessing possible risks. For example, must the impact of pieces of content posted by individual users be considered in the same terms as the activity of the account managed by editorially managed media outlets?

In addition to this, authorities designated by the proposal to oversee platforms' decisions in this area may have the capacity to assess the procedures and practices incorporated by platforms in the fulfillment of these "duties of care". However, can these authorities be entrusted, or better yet, do they have the legitimacy to make comprehensive judgements regarding the desirable openness and plurality of the public discourse, the fairness of the electoral process or the protection of public security? Aren't these matters at the core of our democracies and don't they therefore require the most open and plural of civic debates and institutional procedures?

## 2.5.2. Mitigation of systemic risks

It is also necessary to refer to the different ways the afore-noted risks may be mitigated, according to Article 27. They include the possible adoption of a wide range of internal content moderation practices (paragraph 1), to be complemented with criteria provided by the European Board for Digital Services and the Commission (paragraph 2) and guidelines provided by the Commission. Recital 68 establishes that "risk mitigation measures (...) should be explored via self- and co-regulatory agreements" (contemplated in Article 35) and in particular that "the refusal without proper explanations by an online platform of the Commission's invitation to participate in the drawing up and application of such a code of conduct could be taken into account, where relevant, when determining whether the online platform has infringed the obligations laid down by this Regulation". Such determination is implemented in particular via enhanced supervision mechanisms in the terms of Article 50.

It should be noted that in many cases the only possible way to deal with systemic risks and/or respect the rules established via the codes may require the use of automated filtering mechanisms. Without prejudice to the transparency obligations included in the DSA regarding the use of such mechanisms, it is important to note here that errors by automated monitoring tools can seriously and irreversibly harm users' fundamental rights to privacy, free expression and information, freedom from discrimination, and fair process. However, the DSA does not contain any clear and binding directive to guide the design and implementation of this type of measures, particularly when it comes to human rights implications. From a more general point of view, there are no specific provisions requiring that platforms' internal and independent processes and audits incorporate a clear, international law-based and thorough human rights impact perspective, particularly in the area now under consideration. In this sense, recital 58 only refers to the fact that mitigation measures "should respect the due diligence requirements of this Regulation and be effective and appropriate for mitigating the specific risks identified and [...] should be proportionate in light of the very large online platform's economic capacity and the need



to avoid unnecessary restrictions on the use of their service, taking due account of potential negative effects on the fundamental rights of the recipients of the service”.

Moreover, in the European model, the establishment of restrictions to the right to freedom of expression by non-legislative bodies is connected to the presence of an independent body not subjected to direct political scrutiny or guidance. The very important role that a non-independent body like the European Commission may play vis-à-vis the articulation and implementation of measures with a clear impact on speech is in contradiction with this model.

Last but not least, the activities and measures undertaken and adopted within the framework of Articles 26 and 27 of the DSA cannot in any case be seen as mere private content policies under the exclusive responsibility of online platforms. They are rather the result of a complex intervention involving public bodies/State authorities (at the national and the EU level). Such intervention takes place *ex ante*, via the rules included in the DSA, and *ex post*, due to the capacity of different public bodies to shape and constrain the different ways platforms deal with systemic risks, which entail the dissemination of and access to far more types of content than merely illegal information. Therefore, in such a context, the proper introduction and application of principles and safeguards regarding the protection of human rights as freedom of expression becomes an unavoidable requirement.

## 2.6. Conclusions

The DSA constitutes a very relevant and comprehensive proposal. It establishes a series of fundamental rules and principles regarding, essentially, the way intermediaries participate in the distribution of online content. It also incorporates new important rights for users and obligations for service providers (particularly VLOPs) in areas such as terms and conditions, transparency requirements, statements of reasons in cases of content removals, complaint-handling systems, and out-of-court dispute settlements, among others.

In many areas, the DSA will represent a reinforcement of the rights of users and speakers, vis-à-vis online intermediaries. However, the confusion regarding the notion of actual knowledge, awareness and their relationship with a possible “active” role played by platforms has not been solved and lives on in the sometimes vague language of the proposal. The importance of counting on a liability regime that provides sufficient legal certainty to platforms and users suggests that these issues may still be the object of thorough attention and lengthy debates during the different phases of the adoption of the Regulation.

In addition to this, duties and responsibilities regarding the assessment and mitigation of systemic risks may have an unnecessary and disproportionate impact on the right to freedom of expression of users, as has been outlined in this paper.



## 3. Regulating the moderation of illegal online content

*Alexandre de Stree, professor of EU law at Namur University and the Namur Digital Institute (NADI), academic co-director at the Centre on Regulation in Europe (CERRE) and chair of the expert group for the EU Observatory on the online platform economy.*

*Michèle Ledger, head of practice at Cullen International and senior researcher at NADI.*

### 3.1. Scope and structure of this chapter

This chapter studies the EU regulatory framework applicable to hosting intermediaries when they moderate online content which is illegal or in breach of their terms and conditions.<sup>24</sup> Each of those concepts are already – or are about to be – defined in EU law: (i) **Hosting intermediaries** comprise all organisations which store information provided by, and at the request of, a recipient of the services;<sup>25</sup> (ii) **Content moderation practices** cover all the measures that intermediaries take to manage content which is in violation of the law or of their terms and conditions as well as to manage their users (e.g. the suspension or termination of the user’s account);<sup>26</sup> (iii) **Illegal content** comprises any information which does not comply with EU or national law, irrespective of the precise subject matter or nature of that law.<sup>27</sup>

On this last concept, it is important to distinguish between: content (i) which violates EU or member state law and hence is illegal according to the proposed DSA definition; (ii) which does not violate a law but violates the terms and conditions of a

---

\* The authors wish to thank Maja Cappello and Francisco Cabrera for their very useful comments and discussions; as always, responsibility for the content of this article is the authors’ alone.

<sup>24</sup> This chapter is partly based on de Stree A. et al., “[Online platforms’ moderation of illegal content online](#)”, study for the European Parliament, 2020. On the rules on content moderation, see Floridi L. and Taddeo M. (eds), *The responsibility of online service providers*, Springer, 2017 and Frosio G. (ed), *The Oxford handbook of online intermediary liability*, Oxford University Press, 2020.

<sup>25</sup> 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 [2000] OJ L 178/1, art.14; <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031>, Proposal of the Commission of 15 December 2020 for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31, COM(2020) 825, Art. 5(1), <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN>.

<sup>26</sup> DSA Proposal, Art. 2(p) defines content moderation as “the activities undertaken by providers of intermediary services aimed at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility and accessibility of that illegal content or that information, such as demotion, disabling of access to, or removal thereof, or the recipients’ ability to provide that information, such as the termination or suspension of a recipient’s account”, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN>.

<sup>27</sup> DSA Proposal, Art. 2(g), <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN>.

platform where it is posted; and (iii) which violates neither a law nor the platform's terms and condition but creates harm to users, especially to the most vulnerable ones (such as minors). Our paper focuses mostly on the EU rules applicable to the moderation of the first category of online content, which is the most heavily regulated and only touches, when needed, on the second and third category of content.<sup>28</sup>

The chapter follows the evolution over the years of the EU regulatory framework as the Internet has increased in importance for the economy and society. At the turn of the century when digital intermediaries were in their infancy, the Internet remained relatively free from state intervention as famously suggested by John Perry Barlow in his 1996 Declaration of Independence of Cyberspace<sup>29</sup> (section 5.2). New rules started to be adopted to cater for particular types of illegal content or particular types of digital intermediaries, marking the beginning of the end of digital exceptionalism (section 5.3). Now, new horizontal rules applicable for all platforms and all content are in the making, indicating the end of cyberspace independence (section 5.4). Although these rules are certainly a step in the right direction, some clarifications and improvements are possible (section 5.5).

## 3.2. The independence of cyberspace: the e-Commerce Directive

In 2000, the e-Commerce Directive established a special liability regime for online intermediary services. As explained by the European Commission,<sup>30</sup> this regime pursued four main objectives: (i) to share responsibility for a safe Internet between all the private actors involved and to promote good cooperation with public authorities – thus, injured parties should notify online platforms about any illegality they observe and online platforms should remove or block access to any illegal material of which they are aware; (ii) to encourage the development of e-Commerce in Europe by ensuring that online platforms do not have an obligation to monitor the legality of all material they store; (iii) to strike a fair balance between the fundamental rights of the several stakeholders, in particular privacy and freedom of expression, freedom to conduct business (for platforms) and the right to property including intellectual property of injured parties;<sup>31</sup> and (iv) to strengthen the digital single market by adopting a common EU standard on liability exemptions, especially at a time when national rules and case law were increasingly divergent.

Thus, the e-Commerce Directive creates an exemption from the national liability regime to which the hosting platform is subject and determines the requirements to be met

---

<sup>28</sup> On online disinformation which is often of the third category, see Chapter 6 of this publication.

<sup>29</sup> <https://www.eff.org/fr/cyberspace-independence>.

<sup>30</sup> Explanatory Memorandum of the Commission of 18 November 1998 for the proposal for a directive on certain legal aspects of electronic commerce in the internal market, COM(1998)586, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:51999PC0427&rid=3>.

<sup>31</sup> As protected by the Charter of Fundamental Rights of the European Union, Articles 7, 8, 11, 16 and 17, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.



by the providers to benefit from such an exemption.<sup>32</sup> A hosting platform can escape liability for illegal material uploaded by users when it “does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent”. Should the platform have such knowledge or awareness, it can however benefit from the liability exemption if it “acts expeditiously to remove or to disable access to the information”. Liability exemptions are horizontal: all types of illegal content or activities are covered (unfair market practices, violation of data protection rules, damage to honour and reputation, etc.), as well as various kinds of liabilities (criminal or civil).<sup>33</sup>

To benefit from the liability exemptions, the hosting platform should also be neutral in the sense that its conduct is, in the words of the Court of Justice, “merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores”.<sup>34</sup> A related issue is whether the e-Commerce Directive disincentivises the online platforms to proactively monitor the legality of the material they host because, if they were to do so, they might lose the benefit of the liability exemption. This is sometimes referred to as the good Samaritan paradox. For instance, a platform carrying out *ex ante* moderation practices could be considered as playing an active role and, therefore, be excluded from the liability exemption. During the public consultations organised by the European Commission on the e-Commerce Directive, online platforms mentioned this legal risk of voluntarily introducing more proactive measures.<sup>35</sup> However, in its Communication of September 2017 on tackling illegal online content, the European Commission considered that voluntary proactive measures “do not in and of themselves lead to a loss of the liability exemption, in particular, the taking of such measures need not imply that the online

---

<sup>32</sup> e-Commerce Directive, Art. 14. On the liability exemption, see Chapter 2 of this publication. Also, Kuczerawy A., *Intermediary liability and freedom of expression in the EU: From concepts to safeguards*, Intersentia, 2018, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031>.

<sup>33</sup> Note that, even when a digital intermediary cannot benefit from the liability exemption, it would not necessarily be considered liable under the applicable legal framework. In this case, the national jurisdiction should determine whether legal requirements applicable in the member state are fulfilled (e.g. negligence under civil law) and, if so, decide that the intermediary should be held liable.

<sup>34</sup> Cases C-236/08 to C-238/08 *Google France v Louis Vuitton*, EU:C:2010:159, <https://curia.europa.eu/juris/liste.jsf?num=C-236/08>; <https://curia.europa.eu/juris/liste.jsf?language=en&num=C-238/08>, and Case C-324/09 *L’Oreal and Others v eBay and Others* EU:C:2011:474, <https://curia.europa.eu/juris/liste.jsf?num=C-324/09>. These cases are well explained in van Hoboken J., Quintais J.P., Poort J. and van Eijk N., “Hosting Intermediary Services and Illegal Content Online”, study for the European Commission, 2018, <https://op.europa.eu/en/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1/language-en>

<sup>35</sup> For the 2011 public consultation: Commission Staff Working Document of 11 January 2012, Online services, including e-Commerce, in the Single Market, SEC(2011) 1641, p.35, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52011SC1641>. For the 2015-2016 consultation, Communication from the Commission of 25 May 2016, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, COM(2016) 288, p. 9, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0288> and Commission Staff Working Document of 10 May 2017 on the Mid-Term Review on the implementation of the Digital Single Market Strategy, SWD(2017) 155, p. 28, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0155&rid=1>.

platform concerned plays an active role which would no longer allow it to benefit from that exemption”.<sup>36</sup>

Another pillar of the e-Commerce Directive consists in the prohibition, for EU member states, on imposing a general obligation on the hosting platforms to monitor the material hosted.<sup>37</sup> The Court of Justice has drawn a blurred line between general monitoring measures and specific monitoring measures, in particular in case of suspected violations of intellectual property rights. The first are prohibited;<sup>38</sup> the second are allowed when a fair balance between the fundamental rights of the different stakeholders is achieved.<sup>39</sup> Although imposing a general obligation to monitor is not allowed, online platforms could decide, on a voluntary basis, to carry out spot checks on the online content. This is not prohibited but by doing this, the online platform could be considered as playing an active role as explained above.

In addition, member states may impose on hosting providers the duty to cooperate with the competent authorities.<sup>40</sup> Two types of duties are possible: spontaneous communication to the authorities or communication at their request. Information related to identification of the user who posted illegal content anonymously could be communicated to the victim of the illegal content (so they may bring a claim against the author) or only to the competent authorities.

The last pillar of the e-Commerce Directive is the encouragement of co- and self-regulation in implementation of the rules and principles of the Directive.<sup>41</sup> In particular, the Directive mentions the importance of involving consumers in drafting codes of conduct to ensure that the rules remain balanced. To ensure the effectiveness of those rules, monitoring implementation of the codes is essential.<sup>42</sup> This provision has led, as explained in the next section, to increasing reliance on co- and self-regulation to tackle certain types of illegal materials which have a very negative impact on society, such as hate speech, child abuse content or terrorist content.

---

<sup>36</sup> Communication of the Commission of 28 September 2017, Tackling Illegal Content Online. Towards an enhanced responsibility for online platforms, COM (2017) 555, p.13, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0555>.

<sup>37</sup> e-Commerce Directive, Art. 15(1). On this, see Husovec M., *Injunctions against intermediaries in the European Union: Accountable but not liable?*, Cambridge University Press, 2017

<sup>38</sup> Case [C-360/10](https://curia.europa.eu/juris/liste.jsf?num=C-360/10) *SABAM v. Netlog* EU:C:2012:85; <https://curia.europa.eu/juris/documents.jsf?num=C-360/10>, Case [C-70/10](https://curia.europa.eu/juris/liste.jsf?num=C-70/10) *Scarlet Extended v. SABAM* EU:C:2011:771, <https://curia.europa.eu/juris/liste.jsf?language=en&num=C-70/10>; Case [C-18/18](https://curia.europa.eu/juris/liste.jsf?num=C-18/18), *Glawischnig-Piesczek v. Facebook Ireland* EU:C:2019:821, <https://curia.europa.eu/juris/liste.jsf?num=C-18/18>.

<sup>39</sup> Case [C-314/12](https://curia.europa.eu/juris/liste.jsf?num=C-314/12) *UPC Telekabel Wien v Constantin Film Verleih GmbH* EU:C:2014:192, <https://curia.europa.eu/juris/liste.jsf?num=C-314/12>; Case [C-484/14](https://curia.europa.eu/juris/liste.jsf?num=C-484/14) *Mc Fadden*, para 96, <https://curia.europa.eu/juris/liste.jsf?num=C-484/14>.

<sup>40</sup> e-Commerce Directive, Art. 15(2), <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031>.

<sup>41</sup> e-Commerce Directive, Art. 16, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031>.

<sup>42</sup> In that regard, the Commission has developed some principles for better self- and co-regulation. These principles relate to the conception of the rules: they should be prepared openly and by as many relevant actors as possible; they should set clear targets and indicators and be designed in compliance with EU and national law. The principles also relate to the implementation of the rules: they should be monitored in a way that is sufficiently open and autonomous, improved in an iterative manner (learning by doing) and non-compliance should be subject to a graduated scale of sanctions.

### 3.3. The beginning of the end: The emerging EU regulatory framework for online content moderation

As the Internet became increasingly important in the economy and influential in society, the EU started to take back control of cyberspace and adopted new rules for content moderation, first focussing on the most harmful illegal content<sup>43</sup> and then on some specific types of digital intermediaries.

#### 3.3.1. Regulation of the moderation of specific types of online content

##### 3.3.1.1. Racist and xenophobic hate speech

Already back in 2008, the EU adopted a Counter-Racism Framework Decision which seeks to combat particularly serious forms of hate speech and provides that member states must ensure that racism and xenophobia are sanctioned by criminal law.<sup>44</sup> However, this Decision does not provide for detailed obligations related to online content moderation practices and more generally, the fragmentation of criminal procedural rules across member states makes it difficult to enforce the Decision effectively.<sup>45</sup>

Therefore, in 2016 at the initiative of the Commission, the main online platforms agreed on an EU Code of Conduct on countering all forms of illegal hate speech online<sup>46</sup> with a series of commitments: (i) drawing users' attention to the types of content not allowed by their community standards/guidelines and specifying that they prohibit the promotion of incitement to violence and hateful behaviour; (ii) putting in place a clear and effective process to review reports/notifications of illegal hate speech in order to remove them or make them inaccessible; reviewing notifications on the basis of the community standards / guidelines and national laws, and reviewing the majority of valid reports within 24 hours; (iii) regularly training online platform staff, particularly in relation to societal developments; (iv) encouraging the reporting of illegal hate speech by experts, including through partnerships with civil society organisations – so that they can potentially act as trusted reporters – and strengthening partnerships and collaboration with these

---

<sup>43</sup> This chapter does not deal with content and material violating IP law as this is covered in Chapter 4 of this publication.

<sup>44</sup> [Council Framework Decision 2008/913/JHA](https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32008F0913) of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, O.J. [2008] L 328/55, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32008F0913>.

<sup>45</sup> Report of the European Commission of 27 January 2014 on the implementation of Council Framework Decision 2008/913 on combating certain forms and expressions of racism and xenophobia by means of criminal law, COM(2014)27, <https://op.europa.eu/en/publication-detail/-/publication/ea5a03d1-875e-11e3-9b7d-01aa75ed71a1>.

<sup>46</sup> The Code is available at:

[https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online\\_en](https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en).



organisations to support them; and (v) strengthening communication and cooperation between online platforms and national authorities, in particular with regard to procedures for submitting notifications; collaborating with other online platforms to improve and ensure the exchange of best practices between them.

While considered a step in the right direction, commentators have pointed towards the following weaknesses: risks of private censorship through the priority application of community standards / guidelines; lack of precision in determining the validity of a notification; absence of appeal mechanisms for users whose content has been withdrawn; absence of a requirement for illegal content to be reported to the competent national authorities when removed on the basis of the community standards / guidelines; and the observation that the 24-hour deadline could either make it impossible for online platforms to meet their commitments or could lead to over-blocking practices.<sup>47</sup>

### 3.3.1.2. Child sexual abuse material

In 2011, the EU adopted the **Child Sexual Abuse and Exploitation Directive** which requires member states to take content removal and blocking measures against websites containing or disseminating child sexual abuse material.<sup>48</sup> Such measures must be based on transparent procedures and provide adequate safeguards, in particular be necessary and proportionate, inform the users on the reasons for restriction and ensure the possibility of judicial redress.<sup>49</sup> In practice, member states have adopted two categories of measures: (i) notice-and-takedown measures with national hotlines to which Internet users can report child sexual abuse material that they find online<sup>50</sup>; and (ii) measures based on national criminal law such as general provisions that allow the seizure of material relevant to criminal proceedings (e.g. material used in the commission of an offence) or more specific provisions on the removal of child sexual abuse material.<sup>51</sup>

In parallel to the efforts made by member states, a series of self-regulatory initiatives were taken by digital intermediaries – often encouraged by the European

---

<sup>47</sup> Quintel T. and Ullrich C., “Self-regulation of fundamental rights? The EU Code of Conduct on Hate Speech, related initiatives and beyond” in Petkova B. and Ojanen T., *Fundamental rights protection online: The future regulation of intermediaries*, Edward Elgar, 2019.

<sup>48</sup> Directive 2011/92 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, O.J. [2011] L 335/1, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093>. The Directive provides at Art. 2, for a broad definition of child sexual abuse material that includes real child pornography that visually depicts a child engaged in real or simulated sexually explicit conduct or virtual child pornography, i.e. computer-generated pornographic material involving children. In general on the EU strategy and rules to fight online child pornography, see Jenay P., “Combating child sexual abuse online”, study for the European Parliament, 2015, [https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL\\_STU\(2015\)536481](https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)536481).

<sup>49</sup> Child Sexual Abuse and Exploitation Directive, Art. 25. Measures may consist in various types of public action, such as legislative, non-legislative, judicial or others.

<sup>50</sup> Moreover, INHOPE, a global umbrella organisation for the hotlines, encourages exchange of expertise, <https://www.inhope.org/EN>.

<sup>51</sup> 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, [https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2016\)872&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2016)872&lang=en).



Commission – to better protect minors and make the Internet a safer place for children.<sup>52</sup> In 2017, the Alliance to Better Protect Minors Online, a multi-stakeholder forum facilitated by the European Commission, was set up in order to address emerging risks that minors face online, such as illegal and harmful content (e.g. violent or sexually exploitative content), conduct (e.g. cyberbullying) and contact (e.g. sexual extortion).<sup>53</sup> It is composed of actors from the entire value chain (device manufacturers, telecom operators, media and online platforms used by children). Its action plan includes the provision of accessible and robust tools that are easy to use, the provision of feedback and notification, the promotion of content classification, and the strengthening of cooperation between the members of the alliance and other parties (such as child safety organisations, governments, education services and law enforcement) to enhance best practice sharing.<sup>54</sup> In an evaluation of this alliance, Ramboll indicates that many commitments are difficult to measure, hence their effectiveness is difficult to assess. It also notes that the effectiveness of the alliance is limited by low public awareness and limited internal knowledge sharing. It therefore recommends increasing public awareness in order to strengthen the external monitoring of the commitments and to incentivise the participants to meet them and to reinforce sharing of good practices between members.<sup>55</sup>

### 3.3.1.3. Terrorist content

Terrorist content was the last type of content to be regulated at the EU level but is now the most strictly regulated. In December 2015 after terrorist attacks in several member states, an EU Internet forum to counter terrorist content online was established among EU interior ministers, high-level representatives of major online platforms (such as Facebook, Google, Microsoft and Twitter), Europol, the EU Counter-Terrorism Coordinator and the European Parliament.<sup>56</sup> One of its goals was to address the misuse of the Internet by terrorist groups and to reduce accessibility to terrorist content online. The forum led to an efficient referral mechanism in particular with the EU Internet Referral Unit of Europol, a shared database with more than 200,000 hashes, which are unique digital fingerprints of terrorist videos and images removed from online platforms.

Then in 2017, the EU adopted the Counter-Terrorism Directive which requires member states to take removal and blocking measures against websites containing or

---

<sup>52</sup> A CEO Coalition to Make the Internet a Better place for Kids was set up in 2011, <https://ec.europa.eu/digital-single-market/en/self-regulation-and-stakeholders-better-internet-kids>, and the ICT Coalition for Children Online was set up in 2012, <http://www.ictcoalition.eu>.

<sup>53</sup> European Commission, Alliance to better protect minors online, <https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online>.

<sup>54</sup> The common action is complemented by individual company commitments with a specific timeline to better protect minors online, see: <https://ec.europa.eu/digital-single-market/en/news/individual-company-statements-alliance-better-protect-minors-online>.

<sup>55</sup> Ramboll, “Evaluation of the implementation of the Alliance to Better Protect Minors Online”, study for the European Commission, 2018, <https://op.europa.eu/en/publication-detail/-/publication/122e3bdd-237b-11e9-8d04-01aa75ed71a1/language-en>.

<sup>56</sup> European Commission press release of 3 December 2015, [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_15\\_6243](https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243).



disseminating terrorist content.<sup>57</sup> These measures must follow transparent procedures and provide adequate safeguards, in particular to ensure that they are limited to what is necessary and proportionate and that users are informed of the reason for the measures. In practice, as with the Child Sexual Abuse and Exploitation Directive, member states have adopted two main types of measures:<sup>58</sup> (i) notice-and-takedown measures, which differ among the member states on several issues such as offences covered, time limits for removal and consequences of non-compliance; and (ii) criminal law measures allowing a prosecutor or a court to order companies to remove content or block content or a website, within a period of 24 or 48 hours.

Finally in 2021, the EU went one step further with the adoption of the Terrorism Content Regulation which imposes duties of care on hosting services providers.<sup>59</sup> In addition to transparency reporting obligations,<sup>60</sup> the main new obligations for these hosting service providers are to (i) remove terrorist content within one hour of receiving a valid removal order stemming from a national competent – not necessarily a judicial – authority;<sup>61</sup> to (ii) preserve for six months removed terrorist content and related data necessary for administrative or judicial review or complaint handling or the prevention, detection, investigation and prosecution of terrorist offences;<sup>62</sup> and to (iii) take specific measures (if they have been previously exposed to terrorist content) to address the dissemination of terrorist material on their services, including by deploying automated detection tools.<sup>63</sup> It is interesting to note that where automated tools are used, safeguards should be put in place in particular through human oversight and verification. Although the specific measures are not precisely defined, platforms must in any case ensure they are targeted and proportionate to the risks of exposure and their size, are applied by taking into account the rights and legitimate interests of users (in particular their fundamental rights) and are applied in a diligent and non-discriminatory manner.

---

<sup>57</sup> Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism, OJ [2017] L 88/6, Article 21, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32017L0541>.

<sup>58</sup> Commission Staff Working Document of 12 September 2018, Impact Assessment Terrorism Content Regulation Proposal, SWD(2018) 408, p. 22, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN>.

<sup>59</sup> Regulation 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, OJ [2021] L 172/79, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0784>. This new Regulation will apply from 7 June 2022. Article 2(1) defines a hosting service provider as “a provider of information society services consisting in the storage of information provided by and at the request of the content provider”.

<sup>60</sup> Terrorism Content Regulation, Art. 7.

<sup>61</sup> *Ibid*, Art. 3. These can either be administrative, law enforcement or judicial authorities provided they fulfil their tasks in an objective and non-discriminatory manner and do not seek or take instructions from any other body in relation to the exercise of the tasks under the regulation (recital 35 and Art. 13).

<sup>62</sup> *Ibid*, Art.6.

<sup>63</sup> *Ibid*, Art. 5.

### 3.3.2. Regulation of moderation by specific types of digital intermediaries: Video-sharing platforms

In addition to the regulation of specific types of online illegal content, the EU also started to regulate moderation practices by a specific type of digital intermediaries. Indeed, the 2018 revision of the Audiovisual Media Services Directive (AVMSD) envisages that video-sharing platforms<sup>64</sup> should take appropriate measures to protect: (i) the general public from online content which violates EU law (i.e., racism and xenophobia, child sexual abuse material and terrorist content); (ii) the general public from other forms of hate speech which violates the principles mentioned in the EU Charter of Fundamental Rights (i.e., sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation); and (iii) minors from content which may violate the law or be harmful and impair their physical, mental or moral development.<sup>65</sup> Although the European Commission had initially foreseen<sup>66</sup> that the chapter on video-sharing platforms should lead to maximum harmonisation, this was changed during the course of adoption of the Directive, and member states are therefore free to introduce more far-reaching obligations for video-sharing platforms.

The AVMSD lists the possible measures to be taken such as. transparent and user-friendly mechanisms to report and flag content; systems through which video-sharing platforms explain to users what effect has been given to the reporting and flagging; easy-to-use systems allowing users to rate content; transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints. The Directive specifies that the measures must be appropriate in the light of the nature of the content, the potential harm, the characteristics of the category of persons to be protected, the rights and legitimate interests at stake (in particular those of the video-sharing platforms and the users having created and/or uploaded the content, as well as the public interest). The measures should also be proportionate, taking into account the size of the video-sharing

---

<sup>64</sup> 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, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02010L0013-20181218>. Article 1(1aa) defines a video-sharing platform service as “a service as defined by Articles 56 and 57 TFEU, where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks (...) and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing.”

<sup>65</sup> Audiovisual Media Services Directive, Art.28b(1). on the new obligations imposed on video-sharing platforms, see Valcke P., ‘The EU regulatory framework applicable to audiovisual media services’, in Garzaniti L. et al. (eds.), *Telecommunications, broadcasting and the Internet. EU Competition law & regulation*, 4th ed., Sweet & Maxwell, 2019, pp. 232-235.

<sup>66</sup> See Explanatory Memorandum to Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning provision of audiovisual media services in view of changing market realities, COM(2016) 287, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A287%3AFIN>.



platform and the nature of the provided service. A national regulatory authority (often the media regulator) should assess the appropriateness of the measures.<sup>67</sup>

According to the European Commission, the requirements of the AVMSD are compatible with the liability exemption of the e-Commerce Directive, as the measures imposed on video-sharing platforms relate to the responsibilities of the provider in the organisational sphere and do not entail liability for any illegal information stored on the online platforms as such.<sup>68</sup> Moreover, the measures imposed on video-sharing platforms cannot lead to any *ex ante* control measures or upload-filtering of content.<sup>69</sup>

### 3.3.3. Regulation for all: A re-interpretation of the e-Commerce Directive

To improve the content moderation practices of all digital intermediaries, the Commission also adopted in 2017 a Communication<sup>70</sup> and then in 2018 a Recommendation<sup>71</sup> setting principles for the providers of hosting services as well as member states to take effective, appropriate and proportionate measures to tackle illegal content online. It sets out the general principles for all types of illegal content online and recommends stricter moderation for terrorist content.

Regarding the notice-and-takedown procedures which were not regulated by the e-Commerce Directive and were very divergent across member states,<sup>72</sup> the Recommendation calls for procedures that: (i) are effective, sufficiently precise and adequately substantiated; (ii) respect the rights of content providers with the possibility of counter-notices and out-of-court dispute settlements; and (iii) are transparent.<sup>73</sup>

Regarding proactive measures taken by the digital intermediaries to find and remove illegal content, the Recommendation encourages appropriate, proportionate and specific measures, which could involve the use of automated means, provided some safeguards are in place, in particular human oversight and verification.<sup>74</sup>

Regarding cooperation, the Recommendation encourages close cooperation with national, judicial and administrative authorities and trusted flaggers with the necessary expertise and determined on a clear and objective basis; it also encourages cooperation

---

<sup>67</sup> Audiovisual Media Services Directive, Art.28b(3)-(7).

<sup>68</sup> Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning provision of audiovisual media services in view of changing market realities, COM(2016) 287.

<sup>69</sup> Audiovisual Media Services Directive, Art.28b(3).

<sup>70</sup> See fn 13.

<sup>71</sup> Recommendation 2018/334 of the European Commission of 1 March 2018 on measures to effectively tackle illegal content online, OJ [2018] L 63/50, <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32018H0334>.

<sup>72</sup> See ICF, Grimaldi Studio Legale, and 21c Consultancy, "Overview of the legal framework of notice-and-action procedures in Member States", study for the European Commission, 2018, <https://op.europa.eu/en/publication-detail/-/publication/a56ceb47-2446-11e9-8d04-01aa75ed71a1>.

<sup>73</sup> Recommendation 2018/334, Points 5-17.

<sup>74</sup> *Ibid*, Points 16-21.



among hosting services providers, in particular smaller ones which may have less capacity to tackle illegal content.<sup>75</sup>

### 3.3.4. Summary of the EU regulatory framework and current practices of online moderation

The table below outlines the EU rules against illegal content online according to the nature of the legal instrument (hard law, soft law, or self-regulation).

**Table 1. EU regulatory framework on moderation of illegal content online**

	Hard law	Soft law	Self-regulation
<b>BASELINE</b> <i>All types of hosting platforms and all types of illegal content online</i>	- Directive 2000/31 on e-Commerce	- Commission Communication (2017) on Tackling <i>Illegal Content Online</i>  - Commission <i>Re commendation 2018/334</i> on measures to effectively tackle illegal content online, Ch. II	
<b>Additional rules for video-Sharing Platforms</b>	- Directive 2010/13 Audiovisual Media Services as amended by Directive 2018/1808		
<b>Additional rules for hate speech</b>	- Council Framework Decision 2008/913 on combating certain forms and expressions of racism and xenophobia		- Code of conduct on illegal hate speech online (2016)
<b>Additional rules for child sexual abuse material</b>	- Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography		- Alliance to Better Protect Minors Online (2017)

<sup>75</sup> *Ibid*, Points 22-28.



	Hard law	Soft law	Self-regulation
<b>Additional rules for terrorist content</b>	- Directive 2017/541 on combating terrorism - Regulation 2021/784 on addressing the dissemination of terrorist content online	- Commission <i>Recommendation 2018/334</i> on measures to effectively tackle illegal content online, Ch. III	- EU Internet Forum (2015)

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

Current practices of online moderation vary according to the type and size of the platforms. They deploy a range of content moderation practices, which may be automated and/or which involve human review processes. Some also deploy prevention measures to make sure that harmful content is not seen by users, for instance by preventing certain users from uploading content or by making sure that minors do not see the content, through age verification or age assurance systems. According to recent research, a majority of platforms do not review content before it is uploaded, but they place the responsibility on the uploader to make sure that the content is compliant with the terms and conditions of the platform by ticking a box to that effect.<sup>76</sup> Most platforms have in place systems to detect content that may be in conflict with its terms and condition through flagging measures (including sometimes by trusted flaggers). Automated moderation is particularly widespread to detect child sexual abuse material and can lead to automatic removal if the illegal content is present (hashed) in a database. However, most other content detected by algorithms is reviewed by human moderators before it is removed. According to the same research, medium and large platforms invest 9% of their annual spend on in-house content moderation and they invest 16% to 29% of their annual spend on developing automated systems.

### 3.4. The end of the independence of cyberspace: The Digital Services Act

As a logical development of the regulatory move initiated 10 years ago, the Commission proposed in December 2020, with the Digital Services Act, new horizontal rules for the moderation of illegal content online applicable to all digital platforms and all content, clearly marking the end of the independence of cyberspace.<sup>77</sup>

<sup>76</sup> Report by Ernst and Young LLP, commissioned by the UK government “Understanding how platforms with videosharing capabilities protect users from harmful content online”, 2021, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1008128/EYUK-000140696\\_EY\\_Report\\_-\\_Web\\_Accessible\\_Publication\\_2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1008128/EYUK-000140696_EY_Report_-_Web_Accessible_Publication_2.pdf).

<sup>77</sup> As often explained by Commissioner Thierry Breton, the current progressive regulation of digital space repeats the previous progressive regulation of the terrestrial and then maritime spaces.

### 3.4.1. The proposed DSA and content moderation

The proposed DSA provides for four main categories of online intermediaries as a series of Russian dolls.<sup>78</sup> As we go from the biggest to the smallest doll, the rules imposed by the DSA become more numerous and stricter.

- (i) The broadest category, the biggest doll, is the **provider of intermediary service**, which covers all providers of mere conduit, caching<sup>79</sup> and hosting services;
- (ii) Then comes the **provider of hosting services** defined as storage of information provided by, and at the request of, a recipient of the service. This category includes the providers of cloud, file-sharing, and webhosting services;
- (iii) Then comes the **online platform** defined as a provider of hosting services which, at the request of a recipient of the service, stores and disseminates to the public information. Such a category includes the providers of marketplaces, social media, app stores, and the collaborative economy;
- (iv) Finally, the smallest doll is the **very large online platform** (VLOP) which is an online platform with at least 45m monthly active users in the EU (i.e., 10% of the EU population). This category includes most of the GAFAM.<sup>80</sup>

Rules on content moderation are scattered throughout the DSA but the approach fits with the logic of the proposal which is to introduce asymmetric rules depending on the type of intermediary (or Russian doll). In terms of the substantive rules, the proposed DSA introduces for the first time in EU law: transparency and due diligence obligations over content moderation practices; harmonised notice-and-action mechanisms with an obligation to motivate removal decisions; and rules on the suspension of accounts while granting rights to users to challenge content moderation decisions. VLOPs are subject to additional rules to ensure more comprehensive public oversight of their content moderation practices.

Before we turn to the rules on content moderation per se, it is important to note that the proposal introduces a so-called good Samaritan clause. It states that digital intermediaries “shall not be deemed ineligible for the exemptions from liability (...) solely because they carry out voluntary own-initiative investigations or other activities aimed at detecting, identifying and removing, or disabling access to, illegal content, or take the necessary measures to comply with the requirements of Union law, including those set out in this Regulation”.<sup>81</sup> However, it has been said that this clause may lead to over-removals since, unlike under the US safe harbour and the US good Samaritan clause,<sup>82</sup> providers are not guaranteed protection if they fail to remove content once they have detected illegal content themselves. To be sure to be shielded from liability for third-party illegal content,

---

<sup>78</sup> Resp. DSA Proposal, Art. 2(f), 2(h) and 25, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN>.

<sup>79</sup> For instance, Internet access providers, domain name registries and wi-fi hotspots.

<sup>80</sup> GAFAM is the name given to the five largest and most dominant companies in the information technology industry of the United States, i.e. Google, Apple, Facebook, Amazon and Microsoft.

<sup>81</sup> DSA Proposal, Art. 6, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN>.

<sup>82</sup> Section 230(c) of the Communications Act of 1934, as amended by the Telecommunications Act of 1996 (47 U.S.C. § 230), <https://www.law.cornell.edu/uscode/text/47/230>.



providers could prefer to remove or disable access to the potentially illegal content, leading potentially to over-removals, which may impact the protection of fundamental rights, and in particular freedom of expression.<sup>83</sup>

## 3.4.2. Asymmetric obligations

### 3.4.2.1. All digital intermediaries: Transparency

All digital intermediaries in scope (technical intermediaries, hosting service providers, online platforms and VLOPs) would need to clearly inform users in their terms and conditions of any restrictions they impose on the use of their services, including their content moderation policies and in particular algorithmic decision-making and human review. Also, service providers would need to act in a diligent, objective, and proportionate manner in applying any restrictions, with due regard to the rights and legitimate interests of all parties involved, including applicable fundamental rights.<sup>84</sup>

On top of this, all intermediaries in scope (except for micro-enterprises) would need to produce annual reports on their content moderation activities, including the number of removal orders received from national authorities or notices received from users or flaggers, how fast they acted, and a detailed overview of their own-initiative content moderation activities (number and type of measures taken) and of the complaints-handling activities.<sup>85</sup>

The obligation becomes stricter for online platforms as they would have to report on any automatic content moderation procedures, by providing information on the purpose, indicators of accuracy and any safeguards applied.<sup>86</sup> VLOPs would need to publish transparency reports more frequently: every six months.<sup>87</sup>

### 3.4.2.2. Hosting intermediaries: Notice-and-action procedures

Hosting service providers would need to put in place notice-and-action systems to allow individuals and entities to notify them of allegedly illegal content.<sup>88</sup> The proposed DSA sets out the elements that need to be included in the notices. When all the elements are present, the provider is deemed to have actual knowledge, potentially triggering liability for third-party illegal content, if the provider fails to take down the illegal content. From receiving the notice, the provider would need to act quickly by sending a confirmation of receipt of the notice to the sender (and of whether automated means of processing or decision-

---

<sup>83</sup> For a detailed discussion on this point, see Chapter 2 of this publication.

<sup>84</sup> DSA Proposal, Art. 12, Ibid.

<sup>85</sup> DSA Proposal, Art. 13, Ibid.

<sup>86</sup> DSA Proposal, Art. 23, Ibid.

<sup>87</sup> DSA Proposal, Art. 33, Ibid.

<sup>88</sup> DSA Proposal, Arts. 14-15, Ibid.



making have been used) and by informing the sender of its decision which must be taken in a timely, diligent, and objective manner, and of the redress possibilities.

Hosting service providers that decide to remove or disable access to content would always need to inform the user at the latest at the time of removal of the decision by providing a statement of reasons, which would have to contain certain elements. These elements are for instance, the facts leading to the decision, if automated means were used, and a reference to legal grounds or to the provider's terms and conditions that were breached. The decisions and statement of reasons would need to be published in a publicly accessible database managed by the European Commission.

### 3.4.2.3. Online platforms: Trusted flaggers, user complaints and account suspension

Obligations become stricter for online platforms which also need to deal with notices submitted by trusted flaggers as a matter of priority and without delay.<sup>89</sup> The status (and revocation) of trusted flaggers would be decided by the Digital Service Coordinator<sup>90</sup> of the member state where the applicant/flagger is established if a number of set conditions are fulfilled. It is important to note that the status of trusted flagger is only foreseen to be awarded to entities and not to individuals.<sup>91</sup>

Online platforms would also need to provide their users with easy means to challenge content moderation decisions. As a first step, they would need to put in place internal complaint handling systems to allow users to complain about content moderation decisions.<sup>92</sup> Complaints would have to be receivable for at least six months following the contested decision. Systems would have to be available electronically, free of charge and be easy to access. Complaints would need to be handled in a timely, diligent, and objective manner and could lead to the reversal of the decision without undue delay. Online platforms would also need to inform complainants without undue delay of their decision and of the possibility of further redress mechanisms. Importantly, these decisions could not be taken by online platforms solely on the basis of automated means.

On top of this, users that have been the subject of a content moderation decision would be allowed to resort to a certified out-of-court dispute procedure to seek redress.<sup>93</sup> The proposed DSA sets out the conditions under which the Digital Service Coordinator would have to certify out-of-court dispute resolution bodies. These conditions are aimed at

---

<sup>89</sup> DSA Proposal, Art.19, Ibid..

<sup>90</sup> Digital Service Coordinators would be responsible for all matters relating to application and enforcement of the DSA in a member state, unless a member state has assigned certain specific tasks or sectors to other competent authorities. The requirements for Digital Service Coordinators are specified in Art. 39 of the DSA Proposal: they must perform their tasks in an impartial, transparent and timely manner; they must have adequate technical, financial and human resources to carry out their tasks; they should act with complete independence and remain free from any external influence; and they should neither seek nor take instructions from any other public authority or any private party.

<sup>91</sup> DSA Proposal, Rec.46, Ibid.

<sup>92</sup> DSA Proposal, Art. 17, Ibid. This covers decisions leading to the removal or disabling of access to information, and the suspension or termination of the service to the recipient, or of the user's account

<sup>93</sup> DSA Proposal, Art. 18, Ibid.

ensuring in particular that the bodies are impartial and independent of the online platforms and that they have the necessary expertise. Online platforms would have to engage in good faith with the selected body and would be bound by the decision taken by the body. If the dispute is settled in favour of the user, the platform would need to reimburse all fees and expenses incurred by the user to settle the decision. Of course, users could also seek redress in court, in accordance with their national law.

Of a different nature but worth noting, recipients of services would also have the right to lodge a complaint against providers (if they infringe the DSA) with the Digital Service Coordinator of the member state where the recipient resides.<sup>94</sup> This is not a dispute resolution mechanism though, since the Digital Service Coordinator only needs to assess the complaint and where appropriate, transmit it to the Digital Services Coordinator of establishment.

The proposed DSA also frames the conditions under which online platforms would be able to suspend the provision of services, in other words to suspend user's accounts.<sup>95</sup> This would only be possible for users that frequently provide manifestly illegal content, that is to say where it is evident to a layperson, without any substantive analysis, that the content is illegal.<sup>96</sup> Suspension could only be temporary and after issuance of a prior warning. Platforms would have to take the decision on a case-by-case basis by taking into account a number of listed circumstances including the gravity, the number of occurrences, and the intention. The terms and conditions of the online platforms would have to set out their policy in this respect, which could contain stricter measures in case of manifestly illegal content related to serious crimes. A similar procedure is also foreseen to suspend the processing of manifestly unfounded complaints and notices. Users would be able to challenge suspension decisions as explained above.

#### 3.4.2.4. Very large online platforms: Systemic risk assessment

Very large online platforms would have to identify, analyse and assess at least once a year any significant systemic risks<sup>97</sup> stemming from their services, including the dissemination of content which violates the law but also content which does not violate the law but is harmful.<sup>98</sup> When doing so, they would have to take into account how their content moderation systems influenced any of the systemic risks. On the basis of the assessment, the VLOPs would need to put in place reasonable, proportionate and effective mitigation measures (such as adapting the content moderation practices) tailored to the specific systemic risks identified. Moreover, the European Commission would be able to issue

---

<sup>94</sup> DSA Proposal, Art. 43, Ibid.

<sup>95</sup> DSA Proposal, Art. 20, Ibid.

<sup>96</sup> DSA Proposal, Rec. 47, Ibid.

<sup>97</sup> Systemic risks are not defined in the DSA Proposal which only provides that three categories of systemic risk should be analysed, DSA Proposal, Art. 26: "(i) the dissemination of illegal content through their services; (ii) any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child (...); (iii) intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service, with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security.", Ibid.

<sup>98</sup> DSA Proposal, Arts. 26-27, Ibid.

general guidelines in relation to specific risks, in particular to present best practices and recommend possible measures.

#### 3.4.2.5. Overseeing content moderation

There are no special rules on the oversight of content moderation by public authorities in the proposed DSA although individual decisions can be challenged via internal complaints, by (certified) out-of-court dispute settlement and also in courts. The designated Digital Service Coordinator of the member state where the intermediary is established would be in charge of ensuring application and enforcement of the DSA, unless special tasks were assigned to other competent authorities.<sup>99</sup> On top of receiving the transparency reports, the Digital Service Coordinator would receive certain powers of investigation such as the power to require providers to deliver information, to carry out on-site inspections and to ask members of staff to provide explanations.

Strengthened rules are also foreseen in relation to the supervision of VLOPs, including the appointment of a compliance officer, the intervention of independent auditors and special rules to access data<sup>100</sup> as well as the possibility for the European Commission to directly regulate the VLOP instead of the Digital Service Coordinator of the member state where the platform is established.<sup>101</sup>

### 3.5. Concluding remarks

The evolution of the EU regulatory framework on the moderation of illegal online content, including its most recent step with the proposed Digital Services Act, is interesting. States are progressively regulating cyberspace, which has become increasingly important for the life of their citizens and businesses, and which has not delivered on the – admittedly naïve – promises of the libertarians.<sup>102</sup> In this endeavour, states could be mindful of preserving the greatest opportunities of the Internet, in particular to enhance the exercise of our fundamental freedoms. In that regard, the approach followed by the EU is also interesting. On the one hand, by introducing procedural accountability obligations, it regulates the process of content moderation and not its results. On the other hand, it tailors the obligations to the risks created by illegal content and by platforms.<sup>103</sup> However, some aspects of the proposed DSA could perhaps be clarified and improved.

---

<sup>99</sup> DSA Proposal, Art. 38, Ibid.

<sup>100</sup> DSA Proposal, Arts. 28, 31 and 32, Ibid.

<sup>101</sup> DSA Proposal, Arts. 50-66, Ibid.

<sup>102</sup> Like Barlow's hope of creating a "civilization of the Mind" more humane and fairer than what states had created before.

<sup>103</sup> In favour of a risk-based approach and asymmetric rules, see among others, Buiten M., de Streel A., and Peitz M., "Rethinking liability rules for online hosting platforms", *International Journal of Law and Information Technology* 28, 2020, pp. 139-166, <https://academic.oup.com/ijlit/issue/28/2>.



### 3.5.1.1. Scope

Content moderation can take place for all kinds of illegal content, with no distinction between manifestly illegal content and other forms of illegal content. However, a different take-down procedure – possibly with accelerated deadlines, enhanced communication channels to public authorities and retention obligations regarding evidence (similar to what is foreseen under the Terrorism Content Regulation) could be envisaged for manifestly illegal content where it is evident to a layperson, without any substantive analysis, that the content is illegal.<sup>104</sup>

Also, clear rules on the territorial scope of application of content moderation decisions are missing. Since illegal content is also defined by reference to national law, content may be illegal according to the legislation of one member state but not by reference to the legislation of another member state. It is therefore important to address the territorial scope of take-down decisions in the DSA since this could lead to over-removal which could jeopardise freedom of expression in certain countries.

### 3.5.1.2. Challenging content moderation decisions

The solution envisaged in the proposed DSA for online platforms is sound in our view because certified out-of-court dispute resolution bodies would be able to reassess and potentially reverse content moderation decisions. The proposal puts in place a number of guarantees, such as independence, but it will be important to correctly inform users of the redress mechanism and to specify deadlines to settle the dispute. As it stands, the proposal only allows “recipients of the service” (i.e. a user of a service) addressed by a content moderation decision to select an out-of-court dispute body to resolve a dispute. This means for instance that associations representing specific interests would not have the right to challenge content moderation decisions.

### 3.5.1.3. Oversight of the use of AI content moderation tools

Aside from the requirement to be transparent on the use of automated content moderation systems, the proposed DSA does not refer to criteria to be met by technology used for the detection of illegal content. Thus any automated content moderation would only be subject to the general EU law applicable to automated systems.<sup>105</sup> It would be helpful if any automated moderation system were bound to comply with the six key requirements proposed by the EU High-Level Expert Group on AI: human agency and oversight; technical

---

<sup>104</sup> Also Frosio G. and Geiger C., “Taking fundamental rights seriously in the Digital Services Act’s platform liability regime”, *European Law Journal*, 2021, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3747756](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3747756).

<sup>105</sup> In particular the need for human oversight when privacy is at stake, 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 (General Data Protection Regulation), OJ [2016] L 199/1, Art. 22) <https://eur-lex.europa.eu/eli/reg/2016/679/oj>, and the possible prohibition of manipulative AI systems, Proposal of the European Commission of 21 April 2021 for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), COM(2021) 206, Art. 5), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>.



robustness and safety; privacy and data governance; transparency, diversity, non-discrimination and fairness; societal and environmental wellbeing; and accountability.<sup>106</sup> Moreover, the VLOPs, which have the data, expertise and financial means to develop automated techniques, may usefully share these technologies with small and medium-sized or new platforms.<sup>107</sup> Finally, it is interesting to see that the UK's Online Safety draft bill specifies that the regulator (Ofcom) will be given the power to require that a service provider uses accredited technology, at least to identify and remove terrorist content and child sexual exploitation if Ofcom has reasonable grounds to believe that the service provider is not removing such content.

#### 3.5.1.4. VLOPs and fundamental rights when moderating content

Given that VLOPs may be considered as organising a “public space”,<sup>108</sup> it may now be time to ask them to respect the fundamental rights enshrined in the Charter of Fundamental Rights of the EU in their content moderation practices.<sup>109</sup> The reference to the fact that online platforms need to have due regard for the rights of all parties involved, including applicable fundamental rights could possibly become a positive duty to respect fundamental rights, which of course will need to be balanced out between each other. The terms and conditions of VLOPs could also be scrutinised *ex ante* by the Digital Services Coordinator and/or the Commission to make sure they respect all applicable legislation.

#### 3.5.1.5. Journalistic content or content edited by audiovisual media service providers

As a contrast to the UK's Online Safety Bill,<sup>110</sup> the proposed DSA does not contain any special treatment in relation to professionally edited content, such as journalistic content or content that is under the editorial responsibility of audiovisual media service providers. The UK Bill specifies that so-called Category 1 services<sup>111</sup> have special duties (to be specified by Ofcom in dedicated codes of conduct) to protect content of democratic importance and

---

<sup>106</sup> European Communication White Paper of 19 February 2020 on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:65:FIN>; High-Level Expert Group on Artificial Intelligence, Ethics Guidelines of 8 April 2019 for Trustworthy AI. See also Terrorism Content Regulation, Art.5(3), <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

<sup>107</sup> European Commission Recommendation 2018/334, Point 28.

<sup>108</sup> Elkin-Koren N. and Perel M., “Guarding the guardians: Content moderation by online intermediaries and the rule of law” in Frosio G. (ed), *The Oxford Handbook of Online Intermediary Liability*, Oxford University Press, 2020, pp. 669-678, <https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198837138.001.0001/oxfordhb-9780198837138-e-34>.

<sup>109</sup> Pollicino O., *Judicial protection of fundamental rights on the Internet: A road towards digital constitutionalism?*, Hart, 2021.

<sup>110</sup> Draft published on 12 May 2021 (Bill CP 405), [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/985033/Draft\\_Online\\_Safety\\_Bill\\_Bookmarked.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf).

<sup>111</sup> Category 1 services are subject to additional rules, and the thresholds to be met will be determined by the minister in charge (the Secretary of State). At least one of the threshold conditions would have to be the number of users.



journalistic content. In particular, the UK draft foresees that a special complaints procedure would need to be put in place in relation to content moderation decisions affecting access to journalistic content,<sup>112</sup> with the terms and conditions of platforms having to specify the importance of freedom of expression when taking content moderation decisions in relation to such content. The recently adopted Terrorism Content Regulation also contains a special carve-out for material disseminated to the public for “educational, journalistic, artistic or research purposes or for the purposes of preventing or countering terrorism, including material which represents an expression of polemic or controversial views in the course of public debate”.<sup>113</sup>

#### 3.5.1.6. Protection of minors and harmful content

With regard to legal but harmful content which could be damaging to minors, the only rules would apply to VLOPs and relate to systemic risk assessments and risk mitigation measures which would need to be taken. These measures are not defined at this stage. Nothing is foreseen in relation to other digital intermediaries, which will mean that this matter will be addressed in the platforms’ terms and conditions, without public intervention. Age verification measures and content rating systems are difficult areas to address at the EU level but leaving this whole area to member state legislation would lead to continued tensions between the member states and could weaken the digital single market. In this regard, it is interesting to note that the revised AVMSD foresees that video-sharing platforms should protect minors from content which may impair their physical, mental or moral development. Also, the UK’s Online Safety Bill which echoes many of the provisions of the proposed DSA foresees that all providers in scope would need to conduct a risk assessment of whether children are likely to access their services and providers will only be able to conclude that it is not possible for children to access a service if robust systems and processes such as age verification are in place.

---

<sup>112</sup> Interestingly, the text defines journalistic content as content generated for the purpose of journalism, and which is “UK-linked”.

<sup>113</sup> Terrorism Content Regulation, Art. 1.3.

## 4. From risk to reward? The DSA's risk-based approach to disinformation

*Tarlach McGonagle, Institute for Information Law (IViR), Amsterdam Law School*

*Katie Pentney, DPhil Candidate in Law, University of Oxford*

### 4.1. Introduction

Disinformation is an increasing phenomenon and concern in society, in regulatory and policy-making circles, and in practice for the multiplicity of actors in the information ecosystem. The Covid-19 pandemic – and accompanying ‘infodemic’<sup>114</sup> – have accentuated the risks posed by disinformation and the harms it can occasion.

Though the problem of disinformation has been identified and acknowledged by states, online platforms and civil society, several battlegrounds of contestation remain, including how to best address it, who bears responsibility for accompanying line-drawing exercises, and what safeguards must be put in place to ensure the free exchange of information and ideas online. This has resulted, to date, in various (and sometimes divergent) approaches at the domestic and regional levels, ranging from self-regulation by online platforms, to co-regulatory approaches, to State-imposed identification and removal measures.

It is into this complex and rapidly evolving regulatory system that the Digital Services Act (DSA) proposal has been introduced.<sup>115</sup> The DSA represents the next generation of content moderation generally in several respects, including preventive and reactive approaches, differentiation in the obligations imposed on online platforms, and the inclusion of efforts to combat and mitigate the risks and harms of ‘lawful but awful’ categories of speech, such as disinformation. This chapter focuses on the DSA’s risk-based approach, which implements heightened due diligence obligations for very large online platforms (VLOPs) in light of their reach, scale and impact-to-risk ratio. Section 1.2 provides an overview of the European regulatory and policy frameworks on disinformation into which the DSA proposal has arrived. Sections 1.3 to 1.5 introduce the key elements of the DSA’s risk-based approach, including the identification of systemic risks, the imposition of mitigation requirements and measures to ensure oversight and accountability. Section 1.6

---

<sup>114</sup> Joint Statement by WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse and IFRC, “Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation”, 2020, <https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation>.

<sup>115</sup> The Digital Services Act package includes both the Digital Services Act and the Digital Markets Act. The focus of this chapter is on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825, 15 December 2020 [hereafter, DSA], <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN>.



offers some preliminary reflections on aspects of the proposal which may benefit from further consideration and reflection.

## 4.2. The disinformation landscape

It is important to clarify at the outset that the DSA is not – and does not purport to be – centrally concerned with disinformation.<sup>116</sup> Nevertheless, as a piece of flagship, modernising regulation for online services in Europe, it is certainly a relevant reference point. The approach taken in this chapter is thus to position the DSA within the broader, complex regulatory and policy framework governing disinformation, before zoning in on selected features of the DSA that are likely to prove most relevant for countering online disinformation. First, though, a brief survey and analysis of the most salient evolving definitions of ‘disinformation’ will help to clarify the scope of the term.

### 4.2.1. Evolving definitions

The argument from truth is one of the most enduring rationales for the protection of freedom of expression. Popularized among others by John Milton in *Areopagitica* and John Stuart Mill in *On Liberty*, this epistemic argument articulates the age-old concern that truth will vanquish falsehood, leading to individual and societal development and enlightenment. The need to counter false news, propaganda and disinformation has been a long-standing preoccupation in international human rights law; these issues were given detailed consideration by the drafters of various international treaties.<sup>117</sup>

Contemporary disinformation is, however, qualitatively and quantitatively different to earlier forms.<sup>118</sup> Its online habitat is an utterly changed information ecosystem with unprecedented opportunities for production, dissemination and amplification. Among the game-changing factors are: the ease with which, and scale on which, disinformation is being produced; the quality and sophistication of the content and output; the speed and effectiveness with which it is being disseminated and amplified; the lasting online presence of disinformation; and the possibilities to remain anonymous while engaging in these processes.

In the online information ecosystem, intermediaries and platforms have emerged as a new generation of information and communication power-brokers. Such is the extent of

---

<sup>116</sup> A simple word-search reveals seven instances of ‘disinformation’, some of which are very cursory references and three of which are references to the (title of the) Code of Practice on disinformation.

<sup>117</sup> For a detailed overview and analysis, see: Richter A., “International Standards and Comparative National Approaches to Countering Disinformation in the Context of Freedom of the Media, Vienna: Office of the OSCE Representative on Freedom of the Media”, 2019, <https://www.osce.org/files/f/documents/2/1/424451.pdf>.

<sup>118</sup> McGonagle T., “Fake news’: False fears or real concerns?”, *Netherlands Quarterly of Human Rights*, 2017, pp. 203-209, <https://journals.sagepub.com/doi/full/10.1177/0924051917738685>.



their influence that some commentators speak of the positions of “digital dominance”<sup>119</sup> enjoyed by a coterie of big tech companies and, more generally, of the “platformization” of society.<sup>120</sup> Due to their gate-keeping functions, intermediaries and platforms can facilitate or obstruct access to the online forums in which public debate is increasingly conducted.<sup>121</sup> Intermediaries with search and/or recommendation functions, typically driven by algorithms, have far-reaching influence on the availability, accessibility, visibility, findability and prominence of particular content. This influence is achieved, in part, through the use of algorithmic personalization (or recommender systems).<sup>122</sup> The operators of social network services, for instance, “possess the technical means to remove information and suspend accounts”, which makes them “uniquely positioned to delimit the topics and set the tone of public debate”.<sup>123</sup> Search engines, for their part, aim to and are able to make information more accessible and prominent. This gives them influence over how people find information and ideas and what kinds of information and ideas they find.<sup>124</sup> All of this has ensured that platforms have clear “discursive significance” in society.<sup>125</sup>

Since 2017, there has been heightened attention to, and engagement with, online disinformation at the European and national levels. At the European level, working definitions of disinformation have been put forward and progressively revised and refined.<sup>126</sup>

---

<sup>119</sup> Moore M. and Tambini D. (Eds.), *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*, Oxford, Oxford University Press, 2018, <https://global.oup.com/academic/product/digital-dominance-9780190845124?cc=nl&lang=en&q=9780190845124#>.

<sup>120</sup> van Dijck J., Poell T. and de Waal M., *The Platform Society: Public Values in a Connective World*, Oxford, Oxford University Press, 2018.

<sup>121</sup> See, for example, Kuczerawy A., *Intermediary Liability and Freedom of Expression in the EU: From Concepts to Standards*, Cambridge, Intersentia, 2018, Chapters 1 and 2.

<sup>122</sup> For further analysis, see: Cobbe J. and Singh J., “Regulating Recommending: Motivations, Considerations, and Principles”, *European Journal of Law and Technology*, 10 (3), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3371830](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3371830).

<sup>123</sup> Leerssen P., “Cut Out By The Middle Man: The Free Speech Implications Of Social Network Blocking and Banning In The EU”, *JIPITEC* 6, 2015, pp 99-119, at 99-100, <https://www.jipitec.eu/issues/jipitec-6-2-2015/4271>.

<sup>124</sup> See generally: van Hoboken J., *Search Engine Freedom. On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines*, Alphen aan den Rijn, The Netherlands, Kluwer Law International, 2012, <https://dare.uva.nl/search?identifier=df2041ce-167d-4e00-9a06-c3937ec5acca>.

<sup>125</sup> Laidlaw E.B., *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility*, Cambridge, Cambridge University Press, 2015, p. 204, <https://www.cambridge.org/core/books/regulating-speech-in-cyberspace/7A1E83C71D0D67D13756594BE3726687>.

<sup>126</sup> An analysis of national approaches is beyond the scope of this chapter, but see, for a detailed overview and analysis: European Regulators Group for Audiovisual Media Services (ERGA), “Notions of disinformation and related concepts”, 2020, <https://erga-online.eu/wp-content/uploads/2021/01/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts.pdf>.

**Figure 2. Working definitions of disinformation**

Source	Definition	Year
Information Disorder report <sup>127</sup>	Information that is false and deliberately created to harm a person, social group, organisation or country.	2017
High Level Expert Group (HLEG) final report <sup>128</sup>	All forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit.	2018
Communication, <sup>129</sup> Code of Practice on Disinformation, <sup>130</sup> Action Plan against disinformation <sup>131</sup>	Verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm.	2018
European Democracy Action Plan <sup>132</sup>	False or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm.	2020
Guidance on Strengthening the Code of Practice <sup>133</sup>	The different phenomena to be addressed, while clearly acknowledging the important differences between them. Disinformation in this sense includes disinformation in the narrow sense, misinformation, as well as information influence operations and foreign interference in the information space, including from foreign actors, where information manipulation is used with the effect of causing significant public harm.	2021

The above table provides a brief overview of the most salient attempts to define ‘disinformation’ in European regulatory and policy-making circles. The table traces the rapid

<sup>127</sup> Wardle C. & Derakhshan H., “Information Disorder: Toward an interdisciplinary framework for research and policy making”, Council of Europe DGI 9, 2017, p. 20, <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c>.

<sup>128</sup> “A multi-dimensional approach to disinformation”, report of the independent High Level Group on fake news and online disinformation, March 2018, p. 11, <https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en>.

<sup>129</sup> European Commission Communication, “Tackling online disinformation: a European approach”, COM 236 final, Brussels, 2018, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236>.

<sup>130</sup> EU Code of Practice on Disinformation, 2018, p. 1, [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=54454](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454).

<sup>131</sup> European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication, Action Plan against Disinformation, JOIN36 final, 2018, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018JC0036>.

<sup>132</sup> European Commission Communication, On the European democracy action plan, COM 790 final, Brussels, 2020, p. 18, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:790:FIN>.

<sup>133</sup> European Commission Guidance on Strengthening the Code of Practice on Disinformation, COM 262 final, Brussels, 2021, p. 5, <https://ec.europa.eu/newsroom/dae/redirection/document/76495>.



evolution and progressive refinement of the definition. A first observation is that there has been a move away from the definitional criterion of intention to cause harm. This element, included in the Information Disorder report and the HLEG final report, was problematic, because it had no etymological basis and it would have entailed evidentiary difficulties (i.e., how to prove intent to cause harm). Subsequent definitions emphasise the intention to deceive and the possibility that “public harm” will be caused. Other definitional emphases reveal prevalent concerns about economic gain (e.g. click-bait) or political motives and (foreign) interference in democratic/electoral processes.

Perhaps the most important upshot of these definitional approaches is that the term has an umbrella character. It covers a range of different types of expression, which are fuelled by different motivations, are spread through different means and have different levels of impact.<sup>134</sup>

Given the persistence of concerns about the possible harmful effects of disinformation, it is important to disaggregate the term and identify specific harms before calibrating appropriate responses. Not all effects are harmful and not all harms are illegal. In fact, most are not illegal and ‘harmful’ should accordingly not be conflated with ‘illegal’. As acknowledged in the DSA Proposal: “There is a general agreement among stakeholders that ‘harmful’ (yet not, or at least not necessarily, illegal) content should not be defined in the Digital Services Act and should not be subject to removal obligations, as this is a delicate area with severe implications for the protection of freedom of expression.”<sup>135</sup> In light of this acknowledgement, the broader regulatory and policy context of the DSA will now be explored to give a sense of how disinformation is governed.

## 4.2.2. Broader regulatory and policy frameworks

The DSA proposal does not contain a single reference to either the Council of Europe or the European Convention on Human Rights (ECHR).<sup>136</sup> These are striking omissions in light of the proposal’s repeated references to the importance of freedom of expression (safeguards). It is, of course, logical to frame the DSA within EU law and useful to explain its consistency with existing and pending EU instruments and initiatives. Nevertheless, given the congruence between the regulatory and policy frameworks of the EU and the Council of Europe, the approaches of both organisations are clearly of mutual relevance.

---

<sup>134</sup> For a neat visualisation of disaggregation of disinformation/fake news’, see: European Association for Viewers’ Interests (EAVI), “Beyond ‘Fake News’ - 10 Types of Misleading News”, Infographic, <https://eavi.eu/beyond-fake-news-10-types-misleading-info/>.

<sup>135</sup> DSA proposal, p. 9.

<sup>136</sup> Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950 (as amended by Protocols Nos. 11, 14 and 15, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16), [https://www.echr.coe.int/Documents/Convention\\_ENG.pdf](https://www.echr.coe.int/Documents/Convention_ENG.pdf).



#### 4.2.2.1. Council of Europe

Over the years, the European Court of Human Rights has developed a large body of case-law that offers robust protection for the right to freedom of expression.<sup>137</sup> In relation to disinformation, notable emphases<sup>138</sup> include a firm commitment to strengthening public debate and, specifically in relation to elections, a recognition that “free elections and freedom of expression, particularly freedom of political debate, together form the bedrock of any democratic system”.<sup>139</sup> The quality, accuracy and reliability of information during election periods are of crucial importance for an informed electorate.<sup>140</sup> The Court has also held that “Article 10 of the Convention as such does not prohibit discussion or dissemination of information received even if it is strongly suspected that this information might not be truthful. To suggest otherwise would deprive persons of the right to express their views and opinions about statements made in the mass media and would thus place an unreasonable restriction on the freedom of expression set forth in Article 10 of the Convention”.<sup>141</sup>

Building on the ECHR and the Court’s case-law, the Council of Europe’s Committee of Ministers has in recent years adopted recommendations to member States on topics such as: media pluralism and transparency of media ownership; the roles and responsibilities of Internet intermediaries, and the human rights impacts of algorithmic systems.<sup>142</sup> In May 2021, the Steering Committee for Media and Information Society (CDMSI) adopted a Guidance Note on best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation.<sup>143</sup>

Draft and ongoing standard-setting work for the Committee of Ministers include focuses on: ensuring a favourable environment for the practice of quality journalism in the digital age; impacts of digital technologies on freedom of expression; and election communication and media coverage of electoral campaigns.<sup>144</sup> Of particular relevance is the Committee of Experts on Media Environment and Reform’s ongoing work on “guiding principles for media and communication governance in order to address the shift from

---

<sup>137</sup> Voorhoof D. et al and McGonagle T. (Ed. Sup.), *Freedom of Expression, the Media and Journalists: Case-law of the European Court of Human Rights*, 6<sup>th</sup> edition, IRIS Themes, European Audiovisual Observatory, Strasbourg, 2021, <https://rm.coe.int/iris-themes-vol-iii-2020-edition-en-28-april-2021-/1680a24eee>.

<sup>138</sup> For more detailed analysis of a wider range of relevant, specific references, see: van Hoboken J., Appelman N., Ó Fathaigh R., Leerssen P., McGonagle T., van Eijk N. & Helberger N., *The legal framework on the dissemination of disinformation through Internet services and the regulation of political advertising*, report for the Ministry of the Interior and Kingdom Relations, Amsterdam, Institute for Information Law (IViR), University of Amsterdam, 2019, Chapter 4, (hereafter, ‘IViR disinformation and political advertising study’), [https://www.ivir.nl/publicaties/download/Report\\_Disinformation\\_Dec2019-1.pdf](https://www.ivir.nl/publicaties/download/Report_Disinformation_Dec2019-1.pdf).

<sup>139</sup> *Bowman v. the United Kingdom*, 19 February 1998, § 42, Reports of Judgements and Decisions 1998-I.

<sup>140</sup> *Orlovskaya Iskra v. Russia*, no. 42911/08, § 110, 21 February 2017. See also the discussion of *Brzeziński v. Poland*, no. 47542/07, 25 July 2019, and other relevant case-law, in IViR disinformation and political advertising study, p. 53.

<sup>141</sup> *Salov v. Ukraine*, no. 65518/01, ECHR 2005-VIII (extracts), para. 113.

<sup>142</sup> For an overview of the adopted texts, see: <https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts>.

<sup>143</sup> See: <https://rm.coe.int/content-moderation-en/1680a2cc18>.

<sup>144</sup> For details of these focuses and activities, see: <https://www.coe.int/en/web/freedom-expression/committees>.



established channels to social networks and of related risks (manipulation of public opinion, lack of public trust, information disorder)".<sup>145</sup>

The foregoing demonstrates an extensive and probing engagement with different dimensions of disinformation through a range of complementary focuses rather than frontal engagement in one single standard-setting instrument. The breadth and depth of this engagement could provide useful guidance for EU regulatory and policy initiatives on similar issues, including the DSA's stated commitment to safeguarding the right to freedom of expression.<sup>146</sup>

#### 4.2.2.2. European Union

The relevant EU regulatory and policy framework comprises various instruments that address different aspects of disinformation in keeping with their respective focuses.<sup>147</sup> The most explicit and detailed engagement with disinformation can be found in the self-regulatory Code of Practice on Disinformation. The Code of Practice was agreed on and signed by representatives of several online platforms, social networking service operators and advertising companies (hereafter "signatories") at the end of September 2018.<sup>148</sup> This initiative was taken in the context of a wider range of efforts by the EU to combat online disinformation, including (around the same time) the Commission's Communication, "Tackling online disinformation: A European approach" (April 2018),<sup>149</sup> and an Action Plan against Disinformation (December 2018).<sup>150</sup>

The main aims of the Code of Practice include:

- Ensuring transparency about sponsored content, in particular political advertising, as well as restricting targeting options for political advertising and reducing revenues for purveyors of disinformation;
- Providing greater clarity about the functioning of algorithms and enabling third-party verification;
- Making it easier for users to discover and access different news sources representing alternative viewpoints;

---

<sup>145</sup> Source: <https://www.coe.int/en/web/freedom-expression/msi-ref>.

<sup>146</sup> For further discussion, see Barata J., "The Digital Services Act and its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations", Plataforma por la Libertad de Información, n.d., <https://libertadinformacion.cc/wp-content/uploads/2021/06/DSA-AND-ITS-IMPACT-ON-FREEDOM-OF-EXPRESSION-JOAN-BARATA-PDLI.pdf>.

<sup>147</sup> See Van Hoboken et al., "The legal framework on the dissemination of disinformation through Internet services and the regulation of political advertising, final report", Chapter 5, 2019, [https://www.ivir.nl/publicaties/download/Report\\_Disinformation\\_Dec2019-1.pdf](https://www.ivir.nl/publicaties/download/Report_Disinformation_Dec2019-1.pdf). See also Chapter 3 of this publication.

<sup>148</sup> EU Code of Practice on Disinformation, 2018, <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>.

<sup>149</sup> European Commission, "Tackling online disinformation: A European approach", COM 236 final, 2018, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236>.

<sup>150</sup> European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication, Action Plan against Disinformation, JOIN36 final, 2018, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018JC0036>.



- Introducing measures to identify and close fake accounts and to tackle the issue of automatic bots;
- Enabling fact-checkers, researchers and public authorities to continuously monitor online disinformation.

The Code of Practice sets out a list of detailed commitments, which are structured around five main pillars: A. Scrutiny of ad placements; B. Political advertising and issue-based advertising; C. Integrity of services; D. Empowering consumers; and E. Empowering the research community. Each signatory chooses the most relevant commitments for its own company – in the light of the services it offers and actions it performs.<sup>151</sup>

The latest and most significant development from the DSA perspective is the process to strengthen the Code of Practice against disinformation. One key aim is to develop it into a co-regulatory instrument, for which the DSA's envisaged approach to addressing systemic risks linked to disinformation (discussed in the next section) will be important. The plans to strengthen the Code of Practice involve addressing a number of horizontal issues: reinforced commitments to achieve the Code's objectives; expanded scope; broadened participation; tailored commitments; (further support for the) European Digital Media Observatory; Rapid Alert System. Specific issues to be addressed in detailed fashion are: scrutiny of ad placements; political advertising and issue-based advertising; integrity of services; empowering users; empowering the research and fact-checking community; and monitoring of the Code.

### 4.3. Introducing the DSA's risk-based approach

With this backdrop in mind, we turn now to the DSA's risk-based approach to content moderation. The approach – particularised in Section 4 of the DSA – aims to address harmful, but lawful, content online. It is differentiated in application and holistic in scope. There are three elements in particular which warrant closer inspection – along the lines of who it applies to; what it requires; and why it has been included.

The DSA places heightened due diligence obligations on so-called 'very large online platforms' (VLOPs), in essence those providing services to 45 million or more monthly active recipients in the Union.<sup>152</sup> While this includes existing 'tech giants', such as Facebook, Twitter and YouTube (Google), the Act seems to contemplate the evolution and rapid expansion of online platforms by including an ongoing review and verification process. In particular, the Digital Services Coordinator<sup>153</sup> must verify online platforms' monthly active recipients at least biannually, and designate (or terminate designations) of VLOP status accordingly.<sup>154</sup>

---

<sup>151</sup> For an overview of the implementation of the Code of Practice, see: <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>.

<sup>152</sup> DSA, Article 25 § 1. The Article also provides a methodology for how to calculate this figure (see Article 25 §§ 2 – 4).

<sup>153</sup> See also Chapter 3 of this publication.

<sup>154</sup> DSA, Article 25 § 4.



But what does this designation require and compel? Under Article 26(1) of the DSA, VLOPs must “identify, analyse and assess” – on at least an annual basis – “any significant risks stemming from the functioning and use made of their services in the Union”.<sup>155</sup> The risk assessment must be specific and differentiated according to the services they provide, and must include specified ‘systemic risks’.<sup>156</sup> In addition to the dissemination of illegal content and “any negative effects for the exercise of fundamental rights”,<sup>157</sup> the assessment must cover:

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

This list is non-exhaustive, and additional systemic risks may specifically be assessed; however, it is this last inclusion that is most relevant to disinformation.<sup>158</sup> While the language appears quite broad, there are important restrictions which may limit its application. In particular, the risk assessment includes only ‘intentional’ manipulations of service, and would seemingly apply to coordinated disinformation networks and campaigns. In addition to the required element of intention, the risk assessment applies only to manipulations with actual or foreseeable negative effects on designated categories of harm – including public health and civic discourse – and democratic pillars such as elections and public security.<sup>159</sup> In this way, the risk assessment is both a product of its time and an attempt to reckon with some of the key concerns within the EU and beyond its borders, including the COVID ‘infodemic’, electoral tampering, and concerted disinformation campaigns targeting vulnerable groups within society.

While the risk assessment envisioned by Article 26(1) is largely outward-looking, Article 26(2) compels VLOPs to look inward. In particular, VLOPs must “take into account” how their business models and design features – such as content moderation, recommender and advertising systems – influence the systemic risks referred to in paragraph 1.<sup>160</sup> This includes “the potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions”.<sup>161</sup> While this latter inclusion is broad enough to encompass content that online platforms want to avoid on their platforms, such as nudity or spam, it may also be relevant for ‘lawful but awful’ speech, such as disinformation.

The final consideration is why these risk assessment obligations were imposed at all. The recitals provide some insight in this regard. The recitals note that VLOPs “are used in a way that strongly influences [...] the shaping of public opinion and discourse” and

---

<sup>155</sup> DSA, Article 26 § 1.

<sup>156</sup> Ibid.

<sup>157</sup> DSA, Article 26 §1 (a) and (b), respectively.

<sup>158</sup> Disinformation may also give rise to ‘negative effects’ for the exercise of freedom of expression, including the public’s right to be ‘properly informed’ (see *Sunday Times v. United Kingdom (no. 1)*, App no 6538/74 (ECHR, 26 April 1979) at § 66.

<sup>159</sup> DSA, Article 26 § 1 (c).

<sup>160</sup> DSA, Article 26 § 2.

<sup>161</sup> Ibid.



highlight the social concerns caused by the advertising-driven business model and design choices of these platforms.<sup>162</sup> The need to govern the ‘new governors’<sup>163</sup> is also mentioned: “In the absence of effective regulation and enforcement, they can set the rules of the game, without effectively identifying and mitigating the risks and the societal and economic harm they can cause”.<sup>164</sup>

There are several takeaways from the definitional elements summarised above, particularly in relation to disinformation. First, the focus on ‘very large’ platforms seems to equate reach with risk. Global platforms such as Facebook and Twitter may allow for greater and swifter dissemination of disinformation. However, disinformation campaigns have also arisen on smaller and peer-to-peer networks, which are not subject to the risk assessment obligations of their larger counterparts.<sup>165</sup> Such disinformation campaigns can also cause a range of harms; their impact can be intense even with limited reach, for example within so-called echo chambers or filter bubbles, especially involving hardened conspiracy theorists. The DSA’s prioritisation of risk assessment and mitigation for very large platforms is understandable, but it only addresses a particular type of systemic risks.

Second, the risk assessment heeds calls for greater focus on context, rather than content.<sup>166</sup> This is evident from the inclusion of both the intention underlying and the negative effects of online manipulation in the third systemic risk category. However, it remains to be seen how VLOPs may assess the particularised risks – and specific context – arising in different member states of the European Union, where disinformation sources and targets may vary.

Finally, disinformation campaigns have been shown to be fast-moving and adaptive,<sup>167</sup> which may pose a challenge for the annual – rather than ongoing or *ad hoc* – and rigid risk assessment procedure. The process simply imposes minimum thresholds, however; VLOPs are free to conduct additional risk assessments, should they see fit, and to broaden the kinds of ‘systemic risks’ to be assessed. Whether and to what extent they will do so remains to be seen.

---

<sup>162</sup> DSA, Recital 56.

<sup>163</sup> See Klonick K., “The New Governors: The People, Rules and Processes Governing Online Speech” *Harvard Law Review* 131 (1598), [https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670\\_Online.pdf](https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf).

<sup>164</sup> DSA, Recital 56.

<sup>165</sup> EU DisinfoLab, position paper: “How the Digital Services Act (DSA) Can Tackle Disinformation”, 2021, p. 2, [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/F2164131\\_en](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/F2164131_en).

<sup>166</sup> Mozilla EU Policy, Mozilla position paper on the EU Digital Services Act, 2021, p. 6, <https://blog.mozilla.org/netpolicy/files/2021/05/Mozilla-DSA-position-paper-.pdf/>. On the importance of context in content moderation generally, see Land M.K. & Hamilton R.J., “Beyond Takedown: Expanding the Toolkit for Responding to Online Hate”, in (Dojcinovic P., ed.) *Propaganda, War Crimes Trials and International Law: From Cognition to Criminality* 143Routledge, 2020, and York J.C. and Zuckerman E., “Moderating the Public Sphere” in (Jørgensen R.F. ed.) *Human Rights in the Age of Platforms* (, MIT Press, 2019).

<sup>167</sup> On the use of smaller, peer-to-peer networks to spread ‘lawful but awful’ speech, see Bevenssee E. and Rebellious Data LLC, “The Decentralized Web of Hate: White Supremacists are Starting to Use Peer-to-Peer Technology. Are we Prepared?”, 2020, <https://rebelliousdata.com/wp-content/uploads/2020/10/P2P-Hate-Report.pdf>.



## 4.4. Mitigating risks

In contrast to the more rigid formulation at the stage of identifying systemic risks, the DSA takes a more flexible, co-regulatory approach to how such risks must be mitigated. The key features – including the mandatory and permissive wording, and the differentiated actors involved – are set out here before highlighting how such measures may apply to disinformation.

The mitigation measures are set out in Article 27 of the Regulation, mandating that VLOPs “put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 26”.<sup>168</sup> While the requirement to put in place mitigation measures is mandatory, the list of measures enumerated to fulfil this requirement is permissive and non-exhaustive. Moreover, the measures encompass a broad conception of ‘mitigation’, from adapting decision-making processes, design features like content moderation and advertising systems and service functions, to strengthening risk detection systems; from cooperating with ‘trusted flaggers’ and other online platforms through codes of conduct and crisis protocols, to targeted measures to limit the display and reach of advertising on the platform itself.<sup>169</sup>

Article 27 also envisions a role in mitigating risks for other actors, including the European Board for Digital Services (comprised of Digital Services Coordinators)<sup>170</sup> and the European Commission. Article 27 § 2 requires that the Board, together with the Commission, publish comprehensive reports which identify and assess the most prominent and recurrent systemic risks reported by VLOPs or identified by other means, as well as best practices for VLOPs to mitigate the systemic risks identified.<sup>171</sup> The reports must be published on an annual basis.<sup>172</sup>

In addition, the Commission “may issue general guidelines on the application of paragraph 1 in relation to specific risks, in particular to present best practices and recommend possible measures”.<sup>173</sup> While the legal force or binding effect of these guidelines remains unclear, and there appears to be broad scope with regard to which ‘specific risks’ might be addressed, there are two caveats which are noteworthy. The first is the requirement that the Commission have “due regard to the possible consequences of the measures on fundamental rights enshrined in the Charter of all parties involved”.<sup>174</sup> Whether this requirement will be of any import or consequence will depend on the level of rigour of the Commission’s engagement. By contrast, the “due regard” requirement is not imposed on VLOPs and is not included in the Board’s annual reporting under Article 27 § 2. The second caveat provides, “When preparing those guidelines, the Commission shall organise public consultations.”<sup>175</sup> The precise nature of these public consultations (how many must be held, what role the public’s feedback ought to play, and the like) remains unclear.

---

<sup>168</sup> DSA, Article 27 § 1.

<sup>169</sup> Ibid.

<sup>170</sup> DSA, Articles 47 and 48.

<sup>171</sup> DSA, Article 27 § 2.

<sup>172</sup> Ibid.

<sup>173</sup> DSA, Article 27 § 3.

<sup>174</sup> Ibid.

<sup>175</sup> Ibid.

However, this inclusion provides an additional layer of public involvement and public oversight, and may ensure that those affected by the DSA's risk assessment process are afforded an opportunity to be heard.

There are several aspects of these provisions which are relevant for disinformation. First, the DSA envisions a co-regulatory approach to risk mitigation which includes multiple stakeholders playing differentiated roles in accordance with their skills and responsibilities. However, in contrast to many of the co- and self-regulatory frameworks which came before, such as the Code of Practice (discussed above), the DSA goes further in requiring certain ends (the adoption of “reasonable, proportionate and effective mitigation measures”) while leaving flexibility in the means employed to achieve them. In this sense, Article 27 reflects a shift of emphasis from conduct to result, from process to output. However, while VLOPs remain, at present, free to determine the measures they will put in place – including whether they are put in place globally or within certain regions or States – the requirements of reasonableness, proportionality and effectiveness, may circumscribe the level of flexibility and permissiveness the language would otherwise suggest.

Second, the requirement that the mitigation measures be “tailored to the specific systemic risks identified pursuant to Article 26” may compel VLOPs to explore new ways and share best practices to address systemic risks, including the spread of disinformation on their platforms, with an urgency and vigour not seen to date. Disinformation poses a complex and nuanced challenge, but the imperative of combating its effects on public discourse and democratic pillars has largely befallen (and befuddled) States. The imposition of mitigation requirements to effectively address systemic risks – including the threats to civic discourse, public health, electoral processes and public security posed by disinformation – makes this a problem to be solved for VLOPs as well, and in the process, may harness the resourcefulness and efficiencies of the private sector.

Finally, the sharing of best practices to mitigate systemic risks – in annual reports by the Board and general guidelines issued by the Commission – may further increase the impacts of the DSA's risk-based approach beyond Europe's shores. Many States are keeping a keen eye on the drafting process, and will no doubt seek to model and import the mitigation measures envisioned, the best practices shared, and the general guidelines issued. Similarly, smaller platforms and peer-to-peer networks not subject to the same due diligence requirements may also take note of and seek to implement best practices to mitigate risks on their platforms. Given the potential reach of the mitigation measures, it is critical that VLOPs, the Board and the Commission consider the potential consequences for fundamental rights of any measures contemplated.



## 4.5. Ensuring oversight and transparency

The DSA rounds out its risk-based approach with provisions dedicated to monitoring, oversight and transparency. Two provisions in particular warrant closer inspection: the audit and reporting requirements set out in Articles 28 and 33, respectively.<sup>176</sup>

By virtue of Article 28, VLOPs shall be subjected to annual audits to assess compliance with, *inter alia*, their obligations to conduct assessments of, and adopt mitigation measures to combat, systemic risks.<sup>177</sup> In addition, the audits will assess compliance with any commitments made by VLOPs under codes of conduct and crisis protocols.<sup>178</sup> To comply with the provision, several benchmarks must be met. In particular, the audits must be performed by organisations which are independent from the VLOP under scrutiny; the organisations must have proven expertise in risk management, technical competence and capabilities; and the organisations must have “proven objectivity and professional ethics, based in particular on adherence to codes of practice or appropriate standards”.<sup>179</sup> In terms of results, the organisations must produce audit reports which include (at a minimum) descriptions of the elements audited and the methodology used, the main findings drawn, and an opinion on whether the VLOPs complied with their obligations and commitments.<sup>180</sup> The opinion must include a ranking of either positive, positive with comments, or negative.<sup>181</sup>

The issuance of a negative audit opinion has two notable implications, the first for the auditing organisation and the second for the VLOP. First, the audit report must then include “operational recommendations on specific measures to achieve compliance”.<sup>182</sup> Second, upon receipt of such a report, the VLOPs “shall take due account of any operational measures addressed to them with a view to take the necessary measures to implement them”.<sup>183</sup> In particular, VLOPs must – within one month of receipt of the recommendations – adopt an audit implementation report, setting out those measures or – in the event they do not implement the recommendations – justifying their reasons for not doing so and setting out any alternative measures to address non-compliance.<sup>184</sup>

The DSA also includes heightened “transparency reporting obligations” for VLOPs under Article 33. VLOPs must make publicly available – and transmit to the Digital Services Coordinator – the elements of the risk-based approach outlined above, including:

- (a) a report setting out the results of the risk assessment under Article 26

---

<sup>176</sup> There are additional elements – including provisions specifically addressing recommender systems as well as data access and scrutiny – but we have chosen to focus on these two requirements specifically, as they flow from the identification and mitigation requirements discussed previously.

<sup>177</sup> DSA, Article 28 § 1 (a). These obligations, set out in Articles 26 and 27, fall within Chapter III of the DSA, to which Article 28 § 1 (a) makes explicit reference.

<sup>178</sup> DSA, Article 28 § 1 (b). The code of conduct is provided for in Articles 35 and 36 (code of conduct) and the crisis protocols in Article 37.

<sup>179</sup> DSA, Article 28 § 2.

<sup>180</sup> DSA, Article 28 § 3.

<sup>181</sup> *Ibid.*

<sup>182</sup> DSA, Article 28 § 3 (f).

<sup>183</sup> DSA, Article 28 § 4.

<sup>184</sup> *Ibid.*



- (b) the risk mitigation measures identified and implemented under Article 27
- (c) the audit report under Article 28(3)
- (d) the audit implementation report under Article 28(4)<sup>185</sup>

These transparency reporting obligations accrue at least annually, and must be met within 30 days following the adoption of the audit implementing report.<sup>186</sup> Exceptions are provided where, for instance, the VLOP considers that publication of the above-noted information may disclose confidential information, cause significant vulnerabilities for the security of its service, undermine public security or harm recipients.<sup>187</sup> However, the VLOP may only remove this information from the published reports; the complete (unredacted) reports must be transmitted to the Digital Services Coordinator and Commission, together with a statement of reasons justifying the removal of the information from public reports.<sup>188</sup>

Taken together, the auditing and transparency requirements provide for external review and oversight of VLOPs' compliance with the risk assessment and mitigation measures. This is a key feature to ensure that VLOPs fulfil their obligations to identify and root out systemic risks from their platforms – including disinformation – and that they do so in a way which is measured, critiqued, and subjected to independent oversight from auditors, the Digital Services Coordinator, the Commission, and – perhaps most importantly – the public. The need for greater oversight and transparency has long been noted,<sup>189</sup> and these mechanisms are a significant step in this regard. In addition, the multi-layered transparency obligations compel VLOPs to not only 'do the work', but to show how they have done so in a timely and reasoned manner.

However, several uncertainties remain about how these mechanisms will operate in practice. In the first place, while independent auditing has become a mainstay in realms previously shielded from regulatory oversight – such as the financial sector and data protection<sup>190</sup> – it is not immediately evident that auditing organisations with the requisite level of (proven) expertise and objectivity yet exist. Given the potential weight of the audit opinion and operational recommendations, such audit organisations may have significant impacts on fundamental rights such as freedom of expression and the right to non-discrimination. In light of this preeminent role, further clarity around the requisite qualifications of auditing organisations may be warranted.

---

<sup>185</sup> DSA, Article 33 § 2.

<sup>186</sup> Ibid.

<sup>187</sup> DSA, Article 33 § 3.

<sup>188</sup> Ibid.

<sup>189</sup> See, generally, UN Human Rights Council, Guiding "Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework", Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, 2011, [https://www.ohchr.org/Documents/Issues/Business/A-HRC-17-31\\_AEV.pdf](https://www.ohchr.org/Documents/Issues/Business/A-HRC-17-31_AEV.pdf). In relation to the transparency of online platforms specifically, see The Santa Clara Principles on Transparency and Accountability in Content Moderation, 2018, <https://www.santaclaraprinciples.org/>.

<sup>190</sup> The EU imposed audit requirements on public interest entities, such as banks, by Regulation in 2014 (Regulation No 537/2014), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0537&from=EN>. The General Data Protection Regulation (GDPR), adopted in 2016, provides for oversight in the form of data protection audits under Article 58 (Regulation 2016/679), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.



In addition, while the measures outlined above provide a greater field of vision into the ‘black box’ of online platforms, and allow for oversight of the risk assessment cycle – from the assessment itself, through the mitigation measures employed, to the implementation of audit recommendations – the timelines provided are remarkably short. This is most striking in the time provided for VLOPs to adopt audit implementation reports setting out the “necessary measures” they are taking to implement any operational recommendations received: they have a maximum of one month to do so.<sup>191</sup> In light of the potential breadth and scope of the audits, and any ensuing recommendations, this may affect the quality of the measures implemented and the success of the process outcomes.

Finally, despite the reporting requirements which provide greater transparency and insight into the inner workings of VLOPs, there remain few enforcement mechanisms where VLOPs fail to fulfil their obligations. For instance, while VLOPs must provide reasons for not implementing operational recommendations, there is no penalty should VLOPs choose to implement only few or none. In this sense, the DSA walks a fine line between imposing heightened due diligence obligations on VLOPs (remedying previous failings of co- and self-regulatory approaches) while operating under the (perhaps misguided) presumption that VLOPs will undertake these new responsibilities in good faith.

## 4.6. Risky business? The risk-based approach in action

As the foregoing sections illustrate, disinformation has proven challenging for states and social media platforms to define, prevent, mitigate and remedy. It is into this thorny landscape that the DSA’s risk-based approach has been introduced. While many aspects of the risk-based approach attempt to grapple with the shortcomings of previous approaches to disinformation, the battlegrounds of contestation have been made ever more apparent following the tabling of the proposal. These lingering questions will need to be considered and addressed to ensure a unified and comprehensive approach to combating disinformation online.

The first – and perhaps most rudimentary – question relates to whether disinformation ought to be addressed by the DSA at all. The Committee on Civil Liberties, Justice and Home Affairs of the European Parliament (LIBE Committee) thinks not: In a Draft Opinion, released in May 2021, the LIBE Committee suggested a series of amendments, including the deletion of the provisions setting out the risk-based approach.<sup>192</sup> The LIBE Committee argued the amendments were necessary to protect freedom of expression and to ensure the DSA addresses only the dissemination of ‘illegal’ rather than ‘harmful’ content.<sup>193</sup> With respect to Article 26, setting out the risk-based approach, the LIBE Committee expressed concern that its requirements “go far beyond illegal content where

---

<sup>191</sup> DSA, Article 28 § 4.

<sup>192</sup> Committee on Civil Liberties, Justice and Home Affairs for the Committee on the Internal Market and Consumer Protection on the proposal for a regulation of the European Parliament and of the Council Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM, 0825, 2021, Amendments 21-24, 28, 29, 91-93, [https://www.europarl.europa.eu/doceo/document/LIBE-PA-692898\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/LIBE-PA-692898_EN.pdf).

<sup>193</sup> *ibid.* Amendment 91, ‘Justification’, p. 64/84.



mere vaguely described allegedly ‘negative effects’ are concerned”.<sup>194</sup> Similar concerns were raised regarding the independent audit requirements set out in Article 28.<sup>195</sup> The amendments put forward by the LIBE Committee suggest that further consideration of the scope and aim(s) of the DSA is necessary, particularly in relation to ‘lawful but awful’ speech, such as disinformation.

In the event the risk-based approach survives the ongoing negotiations and debate, a further consideration arises: namely, whether appropriate balances have been struck in the approach taken and substantive requirements put forward in the proposal. Certain civil society organisations have applauded the DSA for its “attempts to strike a careful balance by restricting content removal – which could impinge on freedom of speech – only to illegal content, whilst ensuring that the full range of impacts on our fundamental rights are dealt with through a procedure of risk assessment and mitigation”.<sup>196</sup> Beyond the general approach, however, some organisations have voiced concern over the specifics, including:

- (a) the vagueness of the “systemic risks” in Article 26 and the “reasonable” and “proportionate” thresholds set out in Article 27
- (b) the limitation of risk assessments to (external) “manipulations of service” to the exclusion of risks posed by platforms’ (internal) design choices
- (c) the amount of discretion left to online platforms (and the European Commission) to decide how to go about mitigating systemic risks.<sup>197</sup>

These and other tensions warrant further consideration, reflection and refinement to ensure that the risk-based approach lives up to its promise and expectations, including overcoming some of the main stumbling blocks of previous efforts to curb disinformation online.

While a risk-based approach to identify, curb and remedy systemic risks is novel in the regulation of online speech and the combating of disinformation online, useful guidance and illustrative examples of how such due diligence mechanisms operate in practice can be found in (comparable) industries like finance and data protection.<sup>198</sup> These industries are similarly situated, in that public oversight has been instituted – and due diligence requirements imposed – to peer into the ‘black box’ through human rights impact

---

<sup>194</sup> Ibid., pp. 64-65/84.

<sup>195</sup> Ibid., Amendment 102, pp. 69-70/84.

<sup>196</sup> Avaaz Position Paper on the Digital Services Act, Disinformation and Freedom of Speech, 2021, p. 1, [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/F2164159\\_en](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/F2164159_en).

<sup>197</sup> Ibid., pp. 9-12. See also Article19, “At a glance: Does the EU Digital Services Act protect freedom of expression” 11 February, 2021, <https://www.article19.org/resources/does-the-digital-services-act-protect-freedom-of-expression/>.

<sup>198</sup> In this regard, see Mozilla Mornings, “Unpacking the DSA’s risk-based approach”, 2021, <https://www.youtube.com/watch?v=tEDJ3nx88MM>.



assessments and audits. These experiences may prove useful when reflecting on the scope and contours of Articles 26 and 28, as well as any pitfalls which should be avoided.<sup>199</sup>

Further guidance on how to design and implement due diligence mechanisms can also be derived from international human rights law, policy and practice. The UN Guiding Principles on Business and Human Rights – the leading international standards on the topic – are complemented (and reflected) in a European context by Recommendation CM/Rec(2016)3 of the Council of Europe’s Committee of Ministers to member States on human rights and business. Certain key concepts have also been repurposed for specific application in the online environment in Recommendation CM/Rec(2018)2 of the Council of Europe’s Committee of Ministers to member States on the roles and responsibilities of Internet intermediaries. These references underscore the importance of positional awareness in this dynamic field: in particular, the need to be clear-sighted regarding the DSA’s relevance for addressing disinformation within a more complex regulatory and policy environment.

## 4.7. Conclusion

The regulation of online speech raises significant concerns from the perspective of fundamental rights, including freedom of expression, non-discrimination and the right to an effective remedy. It has proven particularly challenging in respect of ‘lawful but awful’ speech, such as disinformation, which may have broader ramifications for the public or democratic pillars.

It is into this web of complexity that the DSA proposal has been introduced. This chapter focused on the DSA’s risk-based approach to combating disinformation. The proposal is a leap forward in terms of its differentiated, holistic and nuanced regulatory approach. This is evident in several respects, as outlined in this chapter. First, the DSA imposes heightened requirements on VLOPs because of their scale and reach, which reflects their capacity to cause or contribute to public harm(s). Second, the approach is comprehensive in that it is preventative and reactive, prescriptive yet flexible. VLOPs are required to identify, mitigate and disclose designated systemic risks on their platforms, but they are afforded certain flexibility in doing so. Finally, the risk-based approach is nuanced in that its provisions address not only (external) systemic risks, but also the role of (internal) business models and design choices.

A series of questions remain, including whether disinformation and other harmful but legal content should be excluded from the DSA altogether. This begs a further question about how to deal with risks caused by disinformation that do not amount to ‘systemic’ risks in the sense of the DSA proposal. The answers to both questions necessarily have to be

---

<sup>199</sup> For instance, in the financial sector, concerns have been raised about the lack of competition and the perception of conflicts of interest. See, e.g., Prettner C., Ruby-Sachs E., Lehrich J. and Palstra N., “Don’t throw out the Digital Services Act’s key accountability tools”, Euractiv, 2021, <https://www.euractiv.com/section/digital/opinion/dont-throw-out-the-digital-services-acts-key-accountability-tools/>; and Clarke A. “Reforming Audit in the Public Interest”, Luminate, 2020, <https://luminategroup.com/posts/blog/reforming-audit-in-the-public-interest>.



shaped by the right to freedom of expression. Proponents of the approach set out in the DSA argue that it will be a significant step forward in identifying and combating risks, ensuring greater transparency and oversight, and moving beyond the 'black box' of content moderation by private companies. Whether it will live up to this promise remains to be seen.



## ***Beyond free speech***

*Copyright is an exception to freedom of expression and information and deserves a separate chapter. There is an important reason for this exception: we as a society want to protect the work and livelihoods of authors and other creative, technical and financial forces that provide us with films, books, music, etc.*

*The European Union regulates copyright through a set of rules that includes the recently adopted Directive on copyright and related rights in the Digital Single Market (DSM). Although the DSA contains rules that affect the enforcement of copyright, *lex specialis derogat legi generali*, the DSM Directive is considered to override the DSA. But again, things are not that simple.*

***Elenora Rosati** provides in the following chapter a detailed presentation of the interplay between EU copyright rules and the DSA.*



# 5. The Digital Services Act and copyright enforcement: The case of Article 17 of the DSM Directive\*

Eleonora Rosati, Stockholm University\*\*

## 5.1. Introduction

In late 2020, the European Commission unveiled its Proposal for a Digital Services Act<sup>200</sup> (hereinafter, DSA Proposal). Once adopted, the Digital Services Act (hereinafter, DSA) may confirm the core principles of the ‘safe harbour’ regime for certain information society service providers (hereinafter, ISPs), as well as the prohibition of general monitoring as currently found, respectively, at Articles 12 to 14 and 15 of the e-Commerce Directive.<sup>201</sup> It may also uphold the removal of any disincentives to proactive behaviours of ISPs in accordance with its “Good Samaritan” approach, as well as enhance fairness, transparency, and accountability with regard to certain digital services’ moderation practices.

At a first and formal glance, the DSA Proposal and the EU copyright framework, including the 2019 Directive on copyright and related rights in the Digital Single Market<sup>202</sup> (hereinafter, DSM Directive) belong to two separate worlds: recital 11 and Article 1(5) of the former expressly state that it shall be without prejudice to EU rules in the copyright and related rights field. It follows that, among other things, the DSM Directive and the regime contained in its Article 17 shall be regarded as *lex specialis* to the DSA (once adopted), on the consideration that they relate specifically to copyright infringements and

---

\* This contribution is based on the presentation that the Author delivered during the “Copyright and the Digital Services Act” webinar on 27 May 2021, as part of the European Audiovisual Observatory’s webinar series *The New Digital Services Act Package: A Paradigm Shift?*.

\*\* Professor of Intellectual Property and Director of the Institute for Intellectual Property and Market Law (IFIM). The Author wishes to thank the European Audiovisual Observatory for the invitation to contribute to its webinar series and IRIS Special. The views expressed here, as well as any errors and omissions, are only attributable to the Author. Email: [eleonora.rosati@juridicum.su.se](mailto:eleonora.rosati@juridicum.su.se)

<sup>200</sup> European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final (“DSA Proposal”), <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN>.

<sup>201</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, pp. 1–16 (“e-Commerce Directive”), <https://eur-lex.europa.eu/eli/dir/2000/31/oj>.

<sup>202</sup> Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130, 17.5.2019, pp. 92–125, <https://eur-lex.europa.eu/eli/dir/2019/790/oj>.



because they apply to a sub-set of online platforms, that is, online content sharing service providers (hereinafter, OCSSPs).<sup>203</sup>

All the above said, however, it would be both superficial and erroneous to think that the DSA will not affect the interpretation and application of Article 17 of the DSM Directive. The eventual shape of the DSA will be of great relevance to *inter alia* determining when the regime in Article 17 applies in the first place, to whom, and how.<sup>204</sup>

This contribution is structured as follows: Section 1 details the background to the DSM Directive and the DSA Proposal and highlights how intertwined their respective histories are; Section 2 provides an outline of the structure and content of Article 17 of the DSM Directive; Section 3 discusses selected examples relating to Article 17 – including the notion of OCSSP, the specific liability mechanism at paragraph 4, safe harbour availability, and the complaint and redress mechanism at paragraph 9 – in order to illustrate how certain provisions of the DSA could be engaged and affect substantially the interpretation and application of these parts of the copyright provision.

### 5.1.1. The shared history of the DSM Directive and the DSA

The DSM Directive represents an ambitious achievement within the broader EU copyright harmonisation framework, which consists of several directives and regulation adopted over a 30-year period.<sup>205</sup> Within this, Article 17 is – without exaggeration – a story apart, with several points of contact with the DSA Proposal.

#### 5.1.1.1. From the Digital Single Market Strategy to the DSM Directive

Further to the 2014 Public Consultation on the Review of EU Copyright Rules,<sup>206</sup> in 2015 the European Commission, led by its then President Jean-Claude Juncker, unveiled its DSM Strategy.<sup>207</sup> This *inter alia* led to the release of a proposal for a new copyright directive in

---

<sup>203</sup> DSA Proposal, Explanatory Memorandum, p. 4, [https://ec.europa.eu/info/sites/default/files/proposal\\_for\\_a\\_regulation\\_on\\_a\\_single\\_market\\_for\\_digital\\_services.pdf](https://ec.europa.eu/info/sites/default/files/proposal_for_a_regulation_on_a_single_market_for_digital_services.pdf).

<sup>204</sup> See also the discussion in Quintais J.P. and Schwemer S.F., “The interplay between the Digital Services Act and sector regulation: how special is copyright?”, 2021, [https://privpapers.ssrn.com/sol3/papers.cfm?abstract\\_id=3841606](https://privpapers.ssrn.com/sol3/papers.cfm?abstract_id=3841606).

<sup>205</sup> The first copyright directive was adopted in 1991: Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, OJ L 122, 1991, pp. 42–46, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31991L0250>. The EU copyright *acquis* may be viewed at <https://digital-strategy.ec.europa.eu/en/policies/copyright-legislation>.

<sup>206</sup> European Commission, “Report on the Responses to the Public Consultation on the Review of the EU Copyright Rules”, 2014, <https://ec.europa.eu/digital-single-market/en/news/modernisation-eu-copyright-rules-useful-documents>.

<sup>207</sup> European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “A Digital Single Market Strategy for Europe”, /\* COM/2015/0192 final \*/, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192>.



2016.<sup>208</sup> Eventually adopted in 2019, the DSM Directive is supported by multiple rationales, including the perceived need to:

- Contribute to the realization and functioning of the internal market through the establishment of a level playing field for copyright works and other protected subject matters and related services;
- Ensure a high level of protection for rightholders and for copyright and related rights, designed to stimulate innovation, creativity, and investment in and production of new content;
- Pursue cultural objectives, including to safeguard cultural diversity, whilst bringing European common cultural heritage to the fore;
- Address the interpretative uncertainties caused by technological advancement and ensure that copyright legislation does not unduly repress it;
- Guarantee the good functioning of and fairness in the marketplaces for copyright works and other protected subject matter; and
- Modernize certain aspects of the EU copyright *acquis* to take account of technological developments and new channels of distribution of protected content in the internal market.

In relation to the provisions of the DSM Directive individually considered, some of the rationales listed above are more relevant and/or prominent than others in justifying EU legislative intervention. With particular regard to the provision in Article 17 (see below at §5.2), the objective of achieving fairness in the marketplace for copyright and protected content and remedy – what in policy jargon has come to be referred to as the “value gap” or “transfer of value” – was the main justification to support legislative intervention (see also recital 61 in the preamble to the DSM Directive).

The notion of “value gap”/“transfer of value” refers to a mismatch between the value that some digital user-uploaded content platforms, it is argued, obtain from the exploitation of protected content and the revenue returned to relevant rightholders. The argument for submitting that such a gap exists is the perceived inconsistent application of the safe harbour rules for hosting providers under Article 14 of the e-Commerce Directive (see below at §5.1.1.2). The resulting uncertainties arguably led certain user-uploaded content platforms to submit that they would have no responsibility and, thus, liability for the hosting and making available of third-party protected content (copyrighted works and other protected subject matter) through their services. As a result, on the one hand, rightholders would not be appropriately compensated for the exploitation of content to which they own the rights; on the other hand, competition in the market would be distorted.<sup>209</sup> This rationale is embodied in recital 61 in the preamble to the DSM Directive, which acknowledges, in the first place, the growing relevance of online content-sharing

---

<sup>208</sup> Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM/2016/0593 final - 2016/0280 (COD), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0593>.

<sup>209</sup> International Federation of the Phonographic Industry, “Global Music Report 2018 – Annual State of the Industry”, 2018, pp. 26-27, <https://www.fimi.it/kdocs/1922703/gmr-2018-ilovepdf-compressed.pdf>. More recently, International Federation of the Phonographic Industry, “Global Music Report 2021 – Annual State of the Industry”, 2021, p. 40, [https://www.ifpi.org/wp-content/uploads/2020/03/GMR2021\\_STATE\\_OF\\_THE\\_INDUSTRY.pdf](https://www.ifpi.org/wp-content/uploads/2020/03/GMR2021_STATE_OF_THE_INDUSTRY.pdf).



services within the increasingly complex online content market. OCSSPs, as defined in Article 2 (see below at §5.3.1), have become a main source of access to content online. On the one hand, they allow for wider access to cultural and creative works, offer opportunities for related industries to develop new business models, and enable diversity and ease of access to content. On the other hand, they also pose challenges when protected content is uploaded without prior authorisation from rightholders. The same recital 61 also acknowledges the legal uncertainty surrounding whether OCSSPs engage in copyright-relevant acts and need to obtain authorisation from rightholders for content uploaded by their users who do not hold any relevant rights to such content, without prejudice to the application of exceptions and limitations provided for in EU law. That uncertainty further affects the ability of rightholders to obtain appropriate remuneration for the use made by OCSSPs of works and other subject matter to which they own the rights.

### 5.1.1.2. From the e-Commerce Directive to the DSA via the CJEU

The e-Commerce Directive was adopted in 2000, upon a proposal from the European Commission.<sup>210</sup> Among other things, it introduced into the EU legal order exemptions from liability (safe harbours) that would only apply to activities of ISPs "of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored" (recital 42). The e-Commerce Directive prohibits member states from imposing general monitoring obligations on ISPs (Article 15), while clarifying that specific monitoring is allowed (recital 47) and that reasonably expected duties of care aimed at detecting and preventing certain types of illegal activities may be also imposed (recital 48).

Over time, the Court of Justice of the European Union (hereinafter, CJEU) has been asked to clarify the interpretation of the safe harbour rules, including the hosting regime in Article 14 and the prohibition of general monitoring in Article 15. With regard to the former, the Court has held that the "active role" that would serve to remove the availability of the hosting safe harbour should be such that the provider has knowledge of, or control over, the information made available by users of its service.<sup>211</sup> The safe harbour protection shall not be available to a hosting provider that "instead of confining itself to providing that service neutrally by a merely technical and automatic processing of the data provided by its customers, plays an active role of such a kind as to give it knowledge of, or control over, those data."<sup>212</sup>

---

<sup>210</sup> Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the Internal Market (1999/C 30/04), <https://op.europa.eu/en/publication-detail/-/publication/28f57798-cdc4-4888-9963-709156ca799b/language-en>.

<sup>211</sup> *L'Oréal*, C-324/09, EU:C:2011:474, at [113] and [116], <https://curia.europa.eu/juris/document/document.jsf?sessionId=4AE027C5620E99132A924DA30F58EDA9?text=&docid=107261&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=837313>.

<sup>212</sup> *Google France*, C-236/08 to C-238/08, EU:C:2008:389, at [114], <https://curia.europa.eu/juris/document/document.jsf?text=&docid=83961&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=837938>; *L'Oréal*, C-324/09, EU:C:2011:474, at [123]. See also *SNB-REACT*, C-521/17, EU:C:2018:639, at [52], <https://curia.europa.eu/juris/document/document.jsf?text=&docid=204736&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=838197>.



Turning to Article 15, the CJEU has been consistent in stating that Article 15 of the e-Commerce Directive only applies to general monitoring obligations and does not concern monitoring obligations "in a specific case".<sup>213</sup> Overall, EU law allows the imposition on hosting providers of specific duties of care and specific monitoring and filtering obligations.<sup>214</sup> It also allows for injunctions, including blocking injunctions,<sup>215</sup> to be issued against intermediaries in accordance with – insofar as copyright is concerned – Articles 8(3) of the InfoSoc Directive<sup>216</sup> and 3 of the Enforcement Directive,<sup>217</sup> to put an end to existing infringements and prevent further ones from occurring.<sup>218</sup> Still specifically with regard to copyright, in *Scarlet*, C-70/10<sup>219</sup> and *Netlog*, C-360/10<sup>220</sup> the CJEU addressed the availability of injunctions that would impose on an information society service provider an obligation to filter to prevent the making available of infringing content. These rulings are narrow in scope and specific in content: what the CJEU found incompatible with EU law in those cases was only a filtering system imposed on a provider that would: (1) filter information which is stored on its servers by its service users; (2) apply indiscriminately to all of those users; (3) operate as a preventative measure; (4) operate exclusively at its own expense; and (5) perdure for an unlimited period, during which it would be able to identify electronic files containing copyright material, with a view to preventing those works from being made available to the public without a licence. In *Ziggo*, C-610/15<sup>221</sup> the CJEU held that liability for unauthorised acts of communication to the public under Article 3 of the InfoSoc Directive arises at least in case of actual and constructive knowledge. In this sense, operators of platforms with a profit-making intention have an *ex ante* reasonable duty of care and are subjected to an *ex post* notice-

---

<sup>213</sup> *Glawischnig-Piesczek*, C-18/18, EU:C:2019:821, at [34], <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=844450>. See also: Opinion of Advocate General Szpunar in *Glawischnig-Piesczek*, C-18/18, EU:C:2019:458, at [41]-[42], <https://curia.europa.eu/juris/document/document.jsf?text=&docid=214686&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=844450>; *L'Oréal*, C-324/09, EU:C:2011:474, at [139]; *Mc Fadden*, C-484/14, EU:C:2016:689, at [87], <https://curia.europa.eu/juris/document/document.jsf?text=&docid=183363&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=844735>.

<sup>214</sup> See also recently *Glawischnig-Piesczek*, C-18/18, EU:C:2019:821, at [47].

<sup>215</sup> Expressly acknowledged in *UPC Telekabel Wien*, C-314/12, EU:C:2014:192, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=149924&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=844925>.

<sup>216</sup> Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, pp. 10–19, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02001L0029-20190606>.

<sup>217</sup> Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157, 2004, OJ L 195, 2004, pp. 16–25, <https://eur-lex.europa.eu/eli/dir/2004/48/corrigendum/2004-06-02/oj>.

<sup>218</sup> *L'Oréal*, C-324/09, EU:C:2011:474, at [141], endorsing the Opinion of Advocate General Jääskinen in *L'Oréal*, C-324/09, EU:C:2010:757, at [182], <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CC0324>.

<sup>219</sup> *Scarlet*, C-70/10, EU:C:2011:771, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=845785>.

<sup>220</sup> *Netlog*, C-360/10, EU:C:2012:85, <https://curia.europa.eu/juris/document/document.jsf?docid=119512&doclang=en>.

<sup>221</sup> *Ziggo*, C-610/15, EU:C:2017:456, <https://curia.europa.eu/juris/liste.jsf?language=en&T.F&num=c-610-15>.



and-takedown system, which would also include an obligation to prevent infringements of the same kind, e.g. by means of re-uploads of the same content. This conclusion is in line with *L'Oréal*, C-324/09, in which the CJEU detailed the obligations of a “diligent economic operator”.<sup>222</sup>

Like the resolution on the Digital Services Act – Improving the functioning of the Single Market,<sup>223</sup> the DSA Proposal is in continuity with the principles and rules contained in the e-Commerce Directive noted above. The provisions in Articles 12 to 15 of the e-Commerce Directive are reproduced in the draft regulation and upheld. The DSA Proposal is also presented as a confirmation of CJEU case law on Articles 12 to 15 of the e-Commerce Directive.<sup>224</sup> With particular regard to safe harbours (see below at §5.3.3), it is stated that they are available “in respect of any type of liability” (recital 17), but also that the DSA would “apply only to intermediary services” (recital 6), irrespective of their place of establishment (whether intra- or extra-EU). All this said, the DSA Proposal also seeks to introduce greater fairness, transparency, and accountability for digital services’ content moderation policies.<sup>225</sup> It also mandates enhanced responsibilities for certain digital services, with specific obligations for “very large platforms” (Chapter III, Section 4). Furthermore, building *inter alia* upon the 2017 Communication Tackling Illegal Content Online and the ‘Good Samaritan’ approach therein,<sup>226</sup> the DSA also seeks to remove disincentives towards proactive behaviours voluntarily taken by ISPs (Article 6),<sup>227</sup> regulates the content of notices (Article 14), introduces transparency obligations (Articles 13 and 23), and contains a framework for the treatment of trusted flaggers (Article 19). These, as will be discussed in the section at §5.3, are all aspects that will be also relevant to the interpretation and application of Article 17 of the DSM Directive.

## 5.2. Structure and content of Article 17 of the DSM Directive

Article 17 is a lengthy and complex provision that targets OCSSPs as a particular type of ISP. The directive defines an OCSSP as “a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its

---

<sup>222</sup> *L'Oréal*, C-324/09, EU:C:2011:474, at [120]-[124].

<sup>223</sup> European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html).

<sup>224</sup> DSA Proposal, Explanatory Memorandum, p. 4.

<sup>225</sup> DSA Proposal, Explanatory Memorandum, pp. 1-2.

<sup>226</sup> European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Tackling Illegal Content Online – Towards an Enhanced Responsibility of Online Platforms”, COM, 2017, 555 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0555>.

<sup>227</sup> This is also consistent with case law, which has acknowledged that “it is economically more efficient to require intermediaries to take action to prevent infringement occurring via their services than it is to require rightholders to take action directly against infringers”: *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch), 2014, at [251].



users, which it organises and promotes for profit-making purposes” (Article 2(6); see below at §5.3.1).

Overall, the provision moves from a twofold assumption: first, that OCSSPs do perform copyright-restricted acts (recital 64 and Article 17(1)) and are therefore required to obtain an authorisation from concerned rightholders; secondly, that the Directive needs to remedy the legal uncertainty surrounding the responsibility and liability regime of OCSSPs. The latter is also required in order to foster the development of the licensing market between rightholders and OCSSPs, in such a way that licensing agreements are fair and keep a reasonable balance between the parties. While rightholders should receive an appropriate remuneration for the use of their works or other subject matter, in keeping with the principle of contractual freedom, they shall be under no obligation to grant an authorisation or to conclude licensing agreements.

In accordance with Article 17(2), the authorisation obtained by OCSSPs shall cover acts carried out by the OCSSP itself, that is, at least the activities described in Article 17(1), and acts of users of its service. With regard to the latter, the authorisation shall cover uploads falling within the scope of Article 3 of the InfoSoc Directive, insofar as the users do not act on a commercial basis or where their activity does not generate significant revenues. Article 17(4)-(6) introduces both a specific liability regime for OCSSPs that have not obtained the authorisation of relevant rightholders pursuant to Article 17(2) and a mitigation of the regime in Article 17 in favour of certain OCSSPs (see below at §5.3.2).

Article 17(3) provides that, since an OCSSP performs an act of communication/making available to the public, the limitation of liability established in Article 14(1) of the e-Commerce Directive shall not apply to the situations covered by Article 17. The exclusion of the hosting safe harbour is a qualified one: first, it only applies to OCSSPs; secondly, as stated, the exclusion only relates to situations covered by Article 17 (see below at §5.3.3).

Article 17(7) states that the cooperation between OCSSPs and rightholders shall not lead to preventing the availability of works or other subject matter uploaded by users, which do not infringe copyright and/or related rights, including – but not limited (the work or other subject matter or parts thereof may not be protected in the first place, e.g. because the term of protection has expired or the relevant requirements for protection are not fulfilled) to – cases where such works or other subject matter are covered by an exception or limitation. Member states are required to introduce or maintain into their own laws exceptions or limitations for the benefit of users when uploading and making available content generated by them on OCSSPs’ services and allowing (i) quotation, criticism, review; and (ii) use for the purpose of caricature, parody or pastiche.

Article 17(8) mandates that the application of Article 17 shall not lead to any general monitoring obligation. Although no reference is expressly made to Article 15(1) of the e-Commerce Directive, that is the provision which is relevant for the interpretation of Article 17(8). This is confirmed by both the legislative history of Article 17 and the fact that the Directive is *inter alia* based upon, and complements, the rules laid down in the e-Commerce Directive (recital 4 and Article 1(2); see below at §5.3.2).

Article 17(9) requires member states to provide that OCSSPs put in place an effective and expeditious complaint and redress mechanism that is available to users of



their services in the event of disputes over the disabling of access to, or the removal of, works or other subject matter uploaded by them. The resulting obligation on OCSSPs shall in any case respect the EU principle of freedom to provide services, including the country of origin principle provided for in Article 3 of the e-Commerce Directive, where applicable (see below at §5.3.4).

Finally, in accordance with Article 17(10) (and recital 71) the Commission is required, as of 6 June 2019 and in cooperation with the member states, to organise stakeholder dialogues to discuss best practices for cooperation between OCSSPs and rightholders. In consultation with OCSSPs, rightholders, users' organisations and other relevant stakeholders, and considering the results of the stakeholder dialogues, the Commission shall issue guidance on the application of Article 17, in particular regarding the cooperation referred to in paragraph 4 therein. The Commission Article 17 Guidance was released on 4 June 2021.<sup>228</sup>

### 5.2.1. Polish challenge to Article 17

By adopting Article 17, the EU legislature sought to balance copyright protection with *inter alia* users' freedom of expression/information. In the view of the Republic of Poland the resulting framework would however unduly favour the former over the latter. As a result, this member state brought an action (C-401/19<sup>229</sup>) before the CJEU against the Parliament and the Council, seeking the annulment of Article 17(4)(b) and Article 17(4)(c), *in fine* (i.e. the part containing the following wording: "and made best efforts to prevent their future uploads in accordance with point (b)") of the Directive. Should the Court find that the contested provisions could not be deleted from Article 17 without substantively changing the rules contained in the remaining provisions of that article, the Republic of Poland requested that the Court annul Article 17 in its entirety.

The action of the Republic of Poland is based on an alleged breach of the right to freedom of expression and information as *inter alia* guaranteed by Article 11 of the EU Charter of Fundamental Rights<sup>230</sup> (hereinafter, the Charter). Specifically, the Republic of Poland submitted that the imposition on OCSSPs of an obligation to make best efforts to ensure the unavailability of specific works and other subject matter, for which the rightholders have provided the relevant and necessary information (Article 17(4)(b)), and to prevent future uploads of protected works or other subject matter, for which the rightholders have submitted a sufficiently substantiated notice (Article 17(4)(c)), make it necessary for those service providers – in order to avoid liability – to carry out prior automatic verification (filtering) of content uploaded online by users, and therefore make

---

<sup>228</sup> European Commission, Communication from the Commission to the European Parliament and the Council – "Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market", Brussels, COM, 2021, 288 final (Commission Article 17 Guidance),

<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1625142238402&uri=CELEX%3A52021DC0288>.

<sup>229</sup> *Republic of Poland v European Parliament and Council of the European Union*, C-401/19 (in progress), <https://curia.europa.eu/juris/liste.jsf?num=C-401/19>.

<sup>230</sup> Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391-407, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.



it necessary to introduce preventive control mechanisms. Such mechanisms would allegedly undermine the essence of the right to freedom of expression and information and fail to comply with the requirement that limitations imposed on that right be proportional and necessary.

In his Opinion on 15 July 2021, Advocate General Saugmandsgaard Øe advised the CJEU to rule that Article 17 is compatible with the Charter and should not be annulled.<sup>231</sup> Specifically, while the Advocate General considered that freedom of expression/information “is undeniably relevant in the present case”<sup>232</sup> and that Article 17 does interfere with it, he concluded that such interference is allowed under Article 52 of the Charter. The Advocate General also considered that Article 17(7)-(9) contains “meaningful safeguards to protect the users of sharing services against measures involving the improper or arbitrary blocking of their content”.<sup>233</sup>

At the time of writing, the case is still pending before the CJEU.

### 5.3. The relationship between Article 17 and the DSA: What is special about it?

Despite the fact that the DSM Directive and its Article 17 are to be formally regarded as *lex specialis* to the DSA Proposal, the truth is – as stated – that the gaps in the construction and application of that provision will indeed need to be filled through the application of the *lex generalis* as found in the DSA, once adopted. The examples presented below at §5.3.1, §5.3.2.1, §5.3.3, and §5.3.4 demonstrate this; the discussion at §5.3.2.2 concerns a situation in which the *lex specialis* character of Article 17 means that the regime adopted therein shall instead prevail over the general regime in the DSA.

#### 5.3.1. Notion of OCSSP: EU establishment, accessibility, and targeting

To fall within the notion of OCSSP, the following, cumulative requirements need to be fulfilled: first, the provider at hand is an ISP; secondly, the provider stores and gives the

---

<sup>231</sup> Opinion of Advocate General Saugmandsgaard Øe in *Republic of Poland v European Parliament and Council of the European Union*, C-401/19, EU:C:2021:613, <https://curia.europa.eu/juris/document/document.jsf?docid=244201&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=2716252>. For a summary and analysis of the Opinion, see Rosati E., “AG Øe advises CJEU to rule that Article 17 is COMPATIBLE with the EU Charter of Fundamental Rights and should not be annulled”, 2021, <https://ipkitten.blogspot.com/2021/07/ag-e-advises-cjeu-to-rule-that-article.html>.

<sup>232</sup> Opinion of Advocate General Saugmandsgaard Øe in *Republic of Poland v European Parliament and Council of the European Union*, C-401/19, at [72].

<sup>233</sup> Opinion of Advocate General Saugmandsgaard Øe in *Republic of Poland v European Parliament and Council of the European Union*, C-401/19, at [157].



public access to a large amount of copyright works or other protected subject matter uploaded by its users, as its main or one of its main purposes; thirdly, the provider organises and promotes for profit-making purposes such content. The notion of OCSSP is evidently a complex one, which raises several questions.<sup>234</sup>

One question is whether there is a requirement that an OCSSP be established in an EU member state for it to fall within the scope of application of the provision, as is the case with other provisions in the DSM Directive.<sup>235</sup> Among other things, an OCSSP is an “information society service”, that is – in accordance with Article 2(5) – a service within the meaning of Article 1(1)(b) of Directive 2015/1535.<sup>236</sup> In turn, that directive defines “service” as any service normally provided for remuneration (which in any case does not need to be paid directly by the end user<sup>237</sup> or all users of the service<sup>238</sup>) that is provided at a distance, by electronic means, and at the individual request of a recipient of services. There is no express requirement that an OCSSP be established in the EU for it to fall under the scope of application of Article 17. One may thus wonder whether simple accessibility of the provider’s service from the EU suffices to trigger the application of the provision.

In light of the rules contained in the DSA Proposal, establishment and/or targeting of the EU public also appear to be required. Despite this, at the time of writing the CJEU has not yet had the specific opportunity to consider targeting in the context of the right of communication to the public, but it has found it to be required with reference to the right of distribution, as well as to the database (*sui generis*) right and in the trade mark field.<sup>239</sup> Based on recital 8 and Article 11 of the DSA Proposal, targeting towards EU territory could be established based on the circumstances at issue, such as the use of a language or a currency generally used in a certain member state, or the possibility of ordering products

---

<sup>234</sup> See the discussion in Rosati E., “Copyright in the Digital Single Market – Article-by-Article Commentary to the Provisions of Directive”, 2019/790, Oxford University Press, Oxford, pp. 315-324.

<sup>235</sup> These are, expressly, Articles 5, 8, 15 and, implicitly, 6 of the DSM Directive.

<sup>236</sup> Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 2015, pp. 1–15, <https://eur-lex.europa.eu/eli/dir/2015/1535/oj>.

<sup>237</sup> *Star Taxi App*, C-62/19, EU:C:2020:980, at [45], [LINK NOT AVAILABLE IN EN YET] referring for support to *Mc Fadden*, C-484/14, EU:C:2016:689, at [41], and *Vanderborght*, C-339/15, EU:C:2017:335, at [36], <https://curia.europa.eu/juris/document/document.jsf?text=&docid=190323&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1482490>. In the same sense, see also Opinion of Advocate General Szpunar in *Star Taxi App*, C-62/19, EU:C:2020:692, at [36],

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=230875&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1482629>.

<sup>238</sup> *Airbnb Ireland*, C-390/18, EU:C:2019:1112, at [46],

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=221791&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1482722>. In the same sense, also Opinion of Advocate General Szpunar in *Airbnb Ireland*, C-390/18, EU:C:2019:336, at [38],

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=213504&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1482722>, referring to *Papasavvas*, C-291/13, EU:C:2014:2209, at [28]-[29], <https://curia.europa.eu/juris/document/document.jsf?text=&docid=157524&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1482961>.

<sup>239</sup> *Donner*, C-5/11, EU:C:2012:370, at [27]-[29],

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=124189&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1483358>; *Football Dataco*, C-173/11, EU:C:2012:642; at [42] and [45], <https://curia.europa.eu/juris/document/document.jsf?text=&docid=128651&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1483486>; *L’Oréal*, C-324/09, EU:C:2011:474, at [61]-[64].



or services, or using a national top level domain. Targeting towards a certain member state could also be derived from the availability of an application in the relevant national application store, from the provision of local advertising or advertising in the language used in that member state, or from the handling of customer relations such as by providing customer service in the language generally used in that member state.

### 5.3.2. The specific liability mechanism of Article 17(4)

As stated, rightholders are under no obligation to authorise OCSSPs to undertake the acts restricted by Article 17(1). Article 17(4) provides that, in the event that an authorisation from a relevant rightholder has not been obtained, OCSSPs may be liable for the storing of and giving public access to the content uploaded by users, when this incorporates third-party copyright works and other protected subject matter. Users may also be liable, unless they have obtained an authorisation in their own right from relevant rightholders or can successfully invoke an exception or limitation, especially – though not solely – one under Article 17(7). This said, Article 17(4) also introduces a mitigated (direct) liability regime or, as recital 66 refers to it, “a specific liability mechanism”, which follows a “tripartite regime: license, block, or takedown/staydown”.<sup>240</sup> The cumulative conditions that need to be satisfied in order to exclude the liability of an OCSSP for the performance of an act of communication/making available to the public in the event that no authorisation has been granted by the relevant rightholder are that the OCSSP in question has:

1. Made best efforts to obtain an authorisation, in line with the rationale of the provision, that is, to foster the development of a licensing market (Article 17(4)(a));
2. Made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific protected works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information (Article 17(4)(b)); and in any event
3. Acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with Article 17(4)(b) (Article 17(4)(c)).

This paragraph of Article 17 has been one of the most widely discussed aspects of the provision (see also above at §1.2.1). Yet, neither its wording nor the Commission Article 17 Guidance exhaust all questions relating to its interpretation and application. In some instances (see below at §5.3.2.1), the *lex specialis* will need to be supplemented by the *lex generalis*; in other situations (see below at §5.3.2.2), the *lex specialis* character of Article 17 means that the *lex generalis* will not find application.

Article 17(8) further mandates that OCSSPs shall provide rightholders, at their request, with adequate information on the functioning of their practices with regard to the cooperation referred to in Article 17(4) and, where licensing agreements are concluded

---

<sup>240</sup> Ginsburg J.C., “A United States perspective on Digital Single Market Directive Article 17”, in Stamatoudi I. – Torremans P. (eds), *EU Copyright Law. A Commentary*, Cheltenham, Edward Elgar, 2021, 2<sup>nd</sup> edn, §19.22.



between OCSSPs and rightholders, information on the use of content covered by the agreements. In any case, the information at hand shall not necessarily be detailed and individualised information for each work or other subject matter identified (recital 68). The guidance on transparency as identified in the 2018 Commission Recommendation of 1 March 2018 on Measures to Effectively Tackle Illegal Content Online, notably the publication of “clear, easily understandable and sufficiently detailed explanations” of OCSSPs’ policies in respect of the removal or disabling of access to the content that they store and the release of regular reports on their activities, is encouraged for adoption also at the national level.<sup>241</sup> All this is in line with what the DSA Proposal requires at its Article 13.

### 5.3.2.1. Article 17(4)(b) in the shade of the DSA

The final formulation of Article 17(4)(b) seeks to address concerns raised in relation to the European Commission’s proposal with regard to the imposition of obligations on what would eventually be named OCSSPs and the need to reconcile those with the prohibition of general monitoring under Article 15 of the e-Commerce Directive. Article 17(4)(b) imposes duties on both OCSSPs and rightholders. The latter, in particular, shall provide the OCSSP in question with the relevant and necessary information. Like Article 17(4)(c), the obligation under point b) therein requires that the information at hand be sufficiently detailed so as to allow the OCSSP to intervene without having to engage in general monitoring.

In its decision in *L’Oréal*, C-324/09, the CJEU ruled that “insufficiently precise or inadequately substantiated”<sup>242</sup> (removal) requests could impose an obligation on the provider to “act expeditiously”. The same approach is mandated under Article 17(4)(b), though – in line with CJEU case law and contrary to the DSA Proposal (see Article 14(2)(b)) – it is not required that notices invariably contain an indication of the relevant URL(s). Recital 66 of the DSM Directive clarifies that the removal/disabling obligation on the side of the OCSSP shall not arise in the event that rightholders fail to provide the relevant and necessary information on their specific works or other subject matter, or where they do not provide any notification concerning the disabling of access to, or the removal of, specific unauthorised works or other subject matter. In such instances, the receiving OCSSP would not be in a position to make best efforts to avoid the availability of unauthorised content on its services, in accordance with high industry standards of professional diligence. Overall, in line with the Commission Article 17 Guidance, the information should, as a minimum, be accurate as regards rights ownership of the particular work or subject matter in question and allow the OCSSP to effectively apply its technological solutions.<sup>243</sup>

Vice versa, upon receiving the relevant and necessary information, the OCSSP in question shall be under an obligation to make best efforts to ensure, expeditiously, the unavailability of the specific works and other subject matter identified in the information

---

<sup>241</sup> European Commission, Commission Recommendation of 1 March 2018 on Measures to Effectively Tackle Illegal Content Online, C(2018) 1177, final, p. 12, <https://eur-lex.europa.eu/eli/reco/2018/334/oj>. See also Commission Article 17 Guidance, p. 16, with specific regard to Article 17(4).

<sup>242</sup> *L’Oréal*, C-324/09, EU:C:2011:474, at [122].

<sup>243</sup> Commission Article 17 Guidance, p. 14.



provided by rightholders. OCSSPs shall enjoy the freedom to decide how to comply with such an obligation of result. Any technology that allows achievement of the objective underpinning the obligation shall be allowed, insofar as it complies with the requirements under Article 17(4)(b), and Article 17(5) and (7)-(9), as well as general EU law principles, including proportionality. A technologically neutral approach is also recommended in the Commission Article 17 Guidance. In practice, OCSSPs are not required to implement the most expensive or sophisticated solution each and every time, but rather to adopt the most appropriate one depending on the relevant circumstances.<sup>244</sup> It may be expected that notices submitted by trusted flaggers shall be processed and acted upon with priority and without delay, also considering the specific and express recognition that these subjects have received in the context of Article 19 of the DSA Proposal.<sup>245</sup>

Whilst no general monitoring obligations may be imposed, also in line with Article 6 of the DSA Proposal, OCSSPs shall be free to implement general monitoring out of their own volition, subject in any case to the respect of Article 17(7) and (9), as well as the principle of proportionality and users' freedom of expression and information as also protected under Article 11 of the Charter.<sup>246</sup> Article 17(5) indicates that, in determining whether the OCSSP has complied with its obligations under paragraph 4, and in light of the principle of proportionality, a number of elements shall be taken into account, including: type, audience and size of the service; type of works or other subject matter uploaded by the users of the service; availability of suitable and effective means and their cost for service providers. All this suggests that the assessment shall be conducted on a case-by-case basis.

### 5.3.2.2. Where the *lex* is actually *specialis*: Article 17(4)(c)

An aspect of Article 17 in which the *lex specialis* character of the provision vis-à-vis the DSA Proposal is apparent is its paragraph 4, lett. (c). While the latter currently details a mere notice-and-action mechanism at its Article 14, the former also mandates a stay-down obligation. Besides complying with the conditions under Article 17(4)(a) and (b), in order to avoid liability under Article 17(1), an OCSSP shall also have to act expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their services, the notified works or other subject matter, and make best efforts to prevent their future uploads in accordance with point b. Recital 66 clarifies that the obligation under Article 17(4)(c) is not limited to the specific works and protected subject matter in respect of which the best efforts were made to obtain a licence (Article

---

<sup>244</sup> Commission Article 17 Guidance, p. 13. But see Opinion of Advocate General Saugmandsgaard Øe in *Republic of Poland v European Parliament and Council of the European Union*, C-401/19, EU:C:2021:613, at [60]-[62].

<sup>245</sup> Also suggesting the need for a special consideration of 'trusted rightholders', albeit prior to the unveiling of the Commission's proposal for a Digital Services Act, see Spindler G., "The Liability system of Art. 17 DSMD and national implementation – Contravening prohibition of general monitoring duties?" *JIPITEC*, 2019, p. 367, [https://www.jipitec.eu/issues/jipitec-10-3-2019/5041/theliability\\_pdf.pdf](https://www.jipitec.eu/issues/jipitec-10-3-2019/5041/theliability_pdf.pdf), and Leistner M., "European copyright licensing and infringement liability under Art. 17 DSM-Directive compared to secondary liability of content platforms in the U.S. – Can we make the new European system a global opportunity instead of a local challenge?" *Zeitschrift für Geistiges Eigentum*, 2020, pp. 198-201, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3572040](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572040).

<sup>246</sup> See clearly *UPC Telekabel Wien*, C-314/12, EU:C:2014:192, at [55]-[57].



17(4)(a) and is not dependent on whether rightsholders have provided the relevant and necessary information available in advance (Article 17(4)(b)).

The language of Article 17(4)(c) owes to CJEU case law. The obligation under point c) requires that the information at hand be sufficiently detailed, without the relevant notice being necessarily URL-based (unlike what appears to be the case under Article 14 of the DSA Proposal), so as to allow the OCSSP to intervene without having to engage in general monitoring.<sup>247</sup> In any case, still in accordance with CJEU case law, the stay-down obligation under Article 17(4)(c) is not necessarily limited to content identical to that in respect of which the notice was submitted: it may also encompass equivalent content, insofar as the receiving OCSSP is not required to carry out an independent assessment.<sup>248</sup>

### 5.3.3. Safe harbour availability

Article 17(3) provides that, since an OCSSP performs an act of communication/making available to the public, the limitation of liability established in Article 14(1) of the e-Commerce Directive (and Article 5 of the DSA Proposal) shall not apply to the situations covered by Article 17. In accordance with recital 65 in the preamble to the DSM Directive, the meaning and effect of Article 17(3) is only to exclude the potential applicability of the hosting safe harbour to OCSSP in relation to copyright-relevant acts falling within the scope of the provision. As a result, the hosting safe harbour remains potentially available in respect of other legal situations. In any case, any such availability shall depend on the provider in question not playing an “active role” in the sense clarified in CJEU case law (see above at §5.1.1.2).<sup>249</sup>

It is apparent that the DSA as eventually adopted and the continued interpretation of its hosting safe harbour by *inter alia* the CJEU will be relevant to understanding when such protection is available in respect of situations not covered by Article 17. It is submitted that, in practice, there will be instances in which it will be difficult to conclude that, on the one hand, an OCSSP plays an “active role” in relation to user-uploaded content under Article 17 but, on the other hand and also considering the very definition of OCSSP, it does not play such a role with regard to the same content that is unlawful for reasons other than

---

<sup>247</sup> *L'Oréal*, C-324/09, EU:C:2011:474, at [122].

<sup>248</sup> *Glawischnig-Piesczek*, C-18/18, EU:C:2019:821, at [41]-[46].

<sup>249</sup> See *YouTube*, C-682/18 and C-683/18, EU:C:2021:503,

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=243241&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1486852>, at [109]. Also noting the relation between the language employed by the CJEU in its case law and the language adopted by EU legislature for Article 17, see Frosio G., “Reforming the C-DSM reform: a user-based copyright theory for commonplace creativity”, *International Review of Intellectual Property and Competition Law*, 2020, p. 717, [https://www.researchgate.net/publication/337462257\\_Reforming\\_the\\_C-DSM\\_Reform\\_a\\_User-Based\\_Copyright\\_Theory\\_for\\_Commonplace\\_Creativity](https://www.researchgate.net/publication/337462257_Reforming_the_C-DSM_Reform_a_User-Based_Copyright_Theory_for_Commonplace_Creativity).



copyright (for instance because such content doesn't just infringe third-party copyrights but is also defamatory).<sup>250</sup>

The interpretation advanced here differs, however, from the one seemingly endorsed by the European Commission in its DSA Proposal (see above at §5.1.1.2) and also advanced by Advocate General Saugmandsgaard Øe in his Opinion in *YouTube*, C-682/18,<sup>251</sup> in which he considered that the hosting safe harbour in Article 14 of the e-Commerce Directive 2000/31 would apply "horizontally, to all forms of liability".<sup>252</sup> All this said, the proposed interpretation is in line with the one recently endorsed by the CJEU in *YouTube*, C-682/18.<sup>253</sup> When finalizing the text of the DSA, the EU legislature will need to accommodate (and comply with) such an approach: the hosting safe harbour is not available irrespective of the type of liability. Instead, it is only available in principle in situations where the OCSSP neither carries direct (primary) liability nor plays an "active role".

### 5.3.4. The complaint and redress mechanism and protection against misuse

Article 17(9) mandates upon member states to provide that OCSSPs put in place an effective and expeditious complaint and redress mechanism that is available to users of their services in the event of disputes over the disabling of access to, or the removal of, works or other subject matter uploaded by them. Recital 70 clarifies that the complaint and redress mechanism shall serve in particular – though not exclusively – users who could benefit from an exception or limitation to copyright in relation to an upload to which access has been disabled or that has been removed. Complaints shall be processed without undue delay and decisions to disable access to or remove uploaded content shall be subjected to human review. Member states are also required to ensure that users have access to a court or another relevant judicial authority to assert the application of an exception or limitation to copyright and related rights.

Besides what is stated at Article 17(8) (see above at §5.3.2), the DSM Directive does not regulate reporting obligations of OCSSPs and the treatment of those who submit unfounded notices with a certain frequency. Again, this is likely to be something in which

---

<sup>250</sup> See also Nordemann J.B., "Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?", 2018, Directorate General for Internal Policies – Policy Department A: Economic and Scientific Policy, IP/A/IMCO/2017-08 - PE 614.207, p. 23; Rosati E., *Copyright and the Court of Justice of the European Union*, Oxford University Press, Oxford, pp. 117-118.

<sup>251</sup> CJEU Advocate General Saugmandsgaard Øe, Opinion in *YouTube*, C-682/18, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228712&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1486852>.

<sup>252</sup> Opinion of Advocate General Saugmandsgaard Øe in *YouTube*, C-682/18 and C-683/18, EU:C:2020:586, at [138] (emphasis in the original; at the time of writing the decision in these joined cases is pending). In the same sense, in scholarly literature: Husovec M., *Injunctions Against Intermediaries in the European Union: Accountable but Not Liable?*, 2017, Cambridge University Press, Cambridge, p. 56, also referring for support to *Papasavvas*, C-291/13, EU:C:2014:2209, and *L'Oréal*, C-324/09, EU:C:2011:474; Angelopoulos C., *European Intermediary Liability in Copyright: A Tort-Based Analysis*, 2017, Wolters Kluwer, Alphen aan den Rijn, p. 68; Riordan J., *The Liability of Internet Intermediaries*, 2016, Oxford University Press, Oxford, §12.11, §§12.01 and 12.37.

<sup>253</sup> *YouTube*, C-682/18 and C-683/18, EU:C:2021:503, in particular at [108].



the *lex generalis* will find application. This is also expressly acknowledged by the Commission Article 17 Guidance. First, the Guidance recommends that, in line with the approach taken in the DSA Proposal, regular reports on the content blocked as a result of the application of automated tools in fulfilment of requests by rightholders are provided by OCSSPs, also to allow member states to monitor the correct application of Article 17 and detect systematic abuses.<sup>254</sup> In respect of the latter, Article 20(2) of the DSA Proposal mandates the temporary suspension of those who frequently submit notices that are manifestly unfounded. All this may also find application in the context of Article 17.

## 5.4. Conclusion

Insofar as the treatment of OCSSPs is concerned, the relationship between the DSM Directive and the DSA Proposal is of a *lex specialis/lex generalis* kind. The DSA Proposal acknowledges this; in turn, the DSM Directive is expressly based upon and complements those rules in the e-Commerce Directive that will be lifted and incorporated in the DSA. It would be however parochial to think that there will be no point of contact and, potentially, interpretative uncertainty and contrast between these instruments. With particular regard to Article 17 of the DSM Directive, the discussion above has provided some examples of where such contact will be likely to arise once the DSA has been adopted. Such contact will require: (a) the application of the DSA rules to determine the very applicability of Article 17 (§5.3.1) or to shape the content of its obligations (§5.3.4); (b) consideration of CJEU case law as also incorporated in the DSA (§5.3.2.1 and §5.3.3); or (c) the application of the *lex specialis* regime in lieu of the *lex generalis* one (§5.3.2.2). In sum, the eventual shape of the DSA will also be, to a significant extent, the shape of Article 17 in its practical applications.

---

<sup>254</sup> Commission Article 17 Guidance, p. 23.



### ***The happy few at the gates of the Internet***

*Size matters. At least, when it comes to the online environment. Actually, some companies have grown so big that they play the role of gatekeepers of the Internet. And whereas matters of size and dominance are normally addressed through competition law, the European Commission considers that these companies are too big to be dealt with via competition law tools only. The DMA introduces a new way of dealing with them: it defines types of behaviour that have to be regarded as abusive if they are applied by predefined actors, the gatekeepers.*

*How this system will play out and interplay with other regulatory instruments is the topic of **Mark D. Cole**'s following chapter.*



## 6. The proposal for a Digital Markets Act (DMA): On gatekeepers, fairness and transparency in the online environment

*Prof. Dr. Mark D. Cole, Institute of European Media Law and University of Luxembourg\**

### 6.1. Introduction

“[E]nsure contestability, fairness and innovation and the possibility of market entry, as well as public interests that go beyond competition or economic considerations” – this ambitious goal has been put forward by the European Commission in the framework of shaping Europe’s digital future.<sup>255</sup> The Proposal for a Regulation on contestable and fair markets in the digital sector, referred to as the Digital Markets Act (hereinafter: DMA Proposal)<sup>256</sup> is one of the main elements for the fulfilment of this aim.

In this context, reference is often made to a ‘level playing field’ between different competitors on the platform market which is commonly understood as a situation in which every market participant has the same chance of succeeding.<sup>257</sup> To achieve this level playing field, the DMA takes a very specific approach: It differentiates the applicable rules by type and size of platforms and imposes higher obligations on very few very large online platforms which have a gatekeeper position between other companies and customers as end-users. Such obligations concern mainly the opening up of their services, prevention of discrimination and ensuring of transparency for the market. The same level of competitiveness is here not achieved by extending (existing or new) rules in the same

---

\* The author is Professor for Media and Telecommunication Law at the University of Luxembourg and Director for Academic Affairs at the Institute of European Media Law (EMR). The contribution is based on the short overview presentation of the DMA proposal at the EAO conference “The new Digital Services Act Package: A paradigm shift?” in February 2021, <https://www.youtube.com/watch?v=eqFLGiTsnFQ>. The author thanks Christina Etteldorf, research associate at the EMR, for her valuable help in preparing this contribution.

<sup>255</sup> Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Shaping Europe’s digital future”, COM/2020/67 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:67:FIN>.

<sup>256</sup> Proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN>. At the time of drafting this report, there have already been discussions on the proposal within the Council (cf. the progress report ST 8807 2021 INIT, [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3AST\\_8807\\_2021\\_INIT](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3AST_8807_2021_INIT)) and a draft report from the Committee on the Internal Market and Consumer Protection was published (cf. COM(2020)0842 - C9-0419/2020 - 2020/0374(COD), [https://www.europarl.europa.eu/doceo/document/IMCO-PR-692792\\_EN.html](https://www.europarl.europa.eu/doceo/document/IMCO-PR-692792_EN.html)). This contribution focuses however on the Commission’s Proposal.

<sup>257</sup> Cambridge Academic Content Dictionary.



manner to comparable market participants, such as, for example, was the case with the AVMS Directive revision in 2007 and 2018 which aligned the legal framework for linear and non-linear services and subsequently in parts for video-sharing services. Rather, following the motto "with great power comes great responsibility", the DMA takes an approach typical for competition law, where certain legal consequences are attached to certain effects that a company has on the functioning of a free and competitive market. However, from the outset it is clear that the DMA proposal is not a sector-specific competition law that would replace regular EU competition law according to Art. 101 et seq. TFEU and the connected intervention powers of the EU Commission. Much to the contrary, they continue to exist independently, but the DMA complements and strengthens competition law by taking an economic policy approach that is not limited to specific situations of markets and players in individual cases, but generally addresses the necessary framework for a functioning of competition in that part of the Digital Single Market that concerns platforms and some of the services offered.

Therefore, the DMA proposal does not constitute an entire paradigm shift but it is a significant step forward that the DMA recognises the convergence of this sector and the need to respond with more flexible and generally applicable rules compared to the rather static ones in the field of competition law that can only be applied in case of concrete risks for the market. This is certainly a step in the right direction, but the DMA will not create the desired level playing field on its own, there will have to be other building stones to contribute to the goal. This concerns competition law as already mentioned, which will still be applied in specific problematic cases<sup>258</sup>, but also the other part of the package presented by the Commission in the form of the Regulation on a Single Market for Digital Services (Digital Services Act[DSA]) and amending Directive 2000/31/EC<sup>259</sup>. This draft legislative act, which with its tiered system of obligations follows the same basic idea of 'more responsibility leads to more obligations' of the DMA, has a different objective in mind but will still – not least because of its rules concerning very large online platforms – together with competition policy solutions contribute to addressing the systemic problems that arise in the platform economy.<sup>260</sup> Lastly, it should not be forgotten that sectoral law already exists; it applies to the platform economy and must remain an essential part of a well-functioning interdependent regulatory architecture.<sup>261</sup>

The diversity of the online environment – from marketplaces and social networks to news and video platforms as well as many other forms of economic activity – is reflective

---

<sup>258</sup> And has already played an important role in safeguarding competition in the platform sector in the past 15 years, cf. e.g. Commission, Decisions of 14.7.2016 case no. 40411, *Google Search* (AdSense); of 15.4.2015, case no. 40099, *Google Android*; of 30.11.2010, case no. 39740, *Google Search* (Shopping). Cf. on this in detail Hoepfner, "Google's (Non-) Compliance with the EU Shopping Decision", 2020, [https://www.hausfeld.com/media/npcjrw2k/final\\_googles\\_-\\_non\\_-\\_compliance\\_with\\_google\\_search\\_-\\_shopping\\_-\\_stand\\_15-12-2020\\_reduced\\_size.pdf?abstract\\_id=3700748](https://www.hausfeld.com/media/npcjrw2k/final_googles_-_non_-_compliance_with_google_search_-_shopping_-_stand_15-12-2020_reduced_size.pdf?abstract_id=3700748).

<sup>259</sup> Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final. The author of this contribution has published an extensive analysis of the DSA proposal in Cole M.D., Etteldorf C. and Ullrich C., "Updating the Rules for Online Content Dissemination", 2021, <https://doi.org/10.5771/9783748925934>.

<sup>260</sup> Communication from the Commission, "Shaping Europe's digital future" (n 255).

<sup>261</sup> Cf. on this generally Cole M.D., Ukrow J. and Etteldorf C., "On the Allocation of Competences between the European Union and its Member States in the Media Sector", 2021, <https://doi.org/10.5771/9783748924975>, Chapter D; examples are (see below) P2B, AVMSD for VSPs.



of the fact that the activities of an increasing number of sectors unfold online or can be seen as active elements of this environment, which can be challenging when deciding on a regulatory approach to each of those sectors or a horizontal solution. When it comes to content that is relevant for the opinion-forming of citizens, the (audiovisual) media sector is still of primary interest. Platforms and other online actors are part of the media distribution chain by serving as dissemination intermediaries between content producers and users on which media rely for accessibility and visibility to and for the users. At the same time they are also competitors to the media, namely for the attention of users and advertising revenues. Many platforms are – in the wording of the DMA Proposal – gatekeepers between media and third parties (both end-users and advertisers) meaning that they are not just an intermediary but a decisive factor when it comes to ensuring a safe, free and pluralistic media online landscape which in turn is an expectation resulting from fundamental rights and values in the European states.<sup>262</sup> Even though the competition law-inspired approach of the DMA proposal has a different emphasis, in the context of the online environment and the role of the gatekeepers, competition law and such instruments have a fundamental rights- and democracy-preserving function, too.<sup>263</sup> In addition, because of the constitutive relevance of media for democratic societies, the impact of gatekeepers on the media in their fulfilment of a public function needs to be considered. This is even more the case when considering that especially audiovisual media services are subject to specific rules due to their role, which is why the creation of a DMA has to respect those special rules.<sup>264</sup>

## 6.2. The DMA in a nutshell

The DMA is an ambitious piece of legislation concerning both the substance and structure of the proposal. A total of 39 provisions and 79 recitals aim to create “contestable and fair markets” in the digital sector, thus primarily addressing competition aspects in relation to so-called ‘core platform services’ (CPS) provided or offered by ‘gatekeepers’ which are designated as such by the Commission. This objective referred to in Art. 1(1) needs to be

---

<sup>262</sup> See on this aspect Cole M.D., Etteldorf C., Ullrich C., Cross-Border Dissemination of Online Content, <https://www.nomos-elibrary.de/10.5771/9783748906438/cross-border-dissemination-of-online-content?hitid=02&search-click>, p. 53 et seq.

<sup>263</sup> One could use the case of the merger of Facebook and WhatsApp as an illustration of this: Whereas in the actual competition law-based approval of the merger by the Commission in 2014, Case No COMP/M.7217, evidently only economic aspects of market power were considered (in addition to the fact that the market situation for messenger apps then was somewhat different to the near-monopoly situation of more recent times), currently in many investigations by authorities in member states the company’s undeniably increased power on the ‘opinion market’, not least through the acquisition of the WhatsApp user base, is being scrutinised – and this includes elements that go beyond considerations of competition law, cf. generally Etteldorf C., “Data ‘Protection’ from a Different Perspective: German Competition Authority Targets Facebook’s Data Usage”, EDPL 2019-2, pp. 238 – 245, <https://doi.org/10.21552/edpl/2019/2/14>.

<sup>264</sup> The author of this contribution has analysed the impact of the DSA and DMA proposal for the broadcasting sector in his legal issue paper “Overview of the impact of the proposed EU Digital Services Act Package on broadcasting in Europe”, 2021, [https://emr-sb.de/wp-content/uploads/2021/06/EMR\\_Legal-Issue-Paper-DSA-DMA-and-Broadcasting.pdf](https://emr-sb.de/wp-content/uploads/2021/06/EMR_Legal-Issue-Paper-DSA-DMA-and-Broadcasting.pdf).



kept in mind throughout an evaluation of the scope and obligations of the proposed rules as well as how they interact or stand beside other applicable rule sets for the digital sector.

In its objectives, the DMA addresses two principles that build on existing competition law. The principle of a contestable market assumes that there are no entry or exit barriers, no sunk costs and a general access to the same level of technology, while the principle of fairness is less precisely delineated and has several dimensions through which attempts have been made to achieve it in recent competition policy.<sup>265</sup> The question of a fair market essentially revolves around preserving businesses' incentives to succeed and ensuring that consumers retain the possibility to choose between competing options, preventing a single actor from having the power to decide whether others can access the market at all.<sup>266</sup> But the DMA goes beyond safeguarding "mere" contestability, for example by ensuring undistorted competition on platforms (Art. 6 (1) (a) and (d) DMA) or preventing the leveraging of market power in the CPS market to other markets (Art. 5 (f), Art. 6 (1) (b) and (f)).<sup>267</sup> The DMA proposal's instruments are not primarily addressed at consumer benefit but for other business parties to help them succeed in the market, which in turn will benefit consumers.<sup>268</sup>

As indicated, although inspired by competition policy, the DMA proposal is not a typical competition law instrument. Art. 1(6) and its accompanying Recital 10 declare explicitly that the DMA pursues an objective that is "complementary to, but different from" competition law, and is without prejudice to it. Consequently, and contrary to what could be expected when it announced an "ex ante competition tool", which was clearly placed in the context of Art. 101 and 102 TFEU in mid-2020<sup>269</sup>, the Commission did not use Art. 103 TFEU or Art. 352 TFEU as a legal basis for the DMA proposal, but the internal market clause of Art. 114 TFEU. The central point of this provision is the establishment and functioning of the internal market and although ensuring unhindered competition is a part of it there is a separate basis established for action of the EU in this field. In the digital internal or single market, which is influenced by a network of sectoral rules for certain types of players,

---

<sup>265</sup> On the background of the underlying economic theories developed in the 1980's by Baumol W.J., Panzar J.C., and Willig R.D., "Contestable Markets: An Uprising in the Theory of Industry Structure"; Reply, in: *The American Economic Review* 73(3), 1983, pp. 491-496) cf. generally Amavilah V.H., Baumol, Panzar, and Willig's "Theory of Contestable Markets and Industry Structure: A Summary of Reactions", [https://mpr.ub.uni-muenchen.de/41974/1/MPRA\\_paper\\_41974.pdf](https://mpr.ub.uni-muenchen.de/41974/1/MPRA_paper_41974.pdf), with explanations and further references. On the principle of fairness specifically Gerard D., "Fairness in EU Competition Policy: Significance and Implications", *Journal of European Competition Law & Practice*, 9(4), 2018, pp. 211–212.

<sup>266</sup> Commission President Ursula von der Leyen illustratively spoke of platforms that may not become "the new Leviathan", Speech at the Lisbon Web Summit 2020, [https://ec.europa.eu/commission/presscorner/detail/en/speech\\_20\\_2266](https://ec.europa.eu/commission/presscorner/detail/en/speech_20_2266).

<sup>267</sup> Schweitzer H., "The Art to Make Gatekeeper Positions Contestable and the Challenge to Know What is Fair: A Discussion of the Digital Markets Act Proposal", 2021. Forthcoming, *ZEUP* (3) 2021, p. 8, <https://ssrn.com/abstract=3837341>.

<sup>268</sup> For a similar approach see also the UK where the newly introduced Digital Markets Unit (DMU) has a broader oversight power which allows the application of instruments for the benefit of business users of platforms but in addition also the direct enforcement of consumer protection rules against these, cf. Competition and Markets Authority, Policy paper, "The CMA's Digital Markets Strategy", February 2021 refresh, Updated 9 February 2021, <https://www.gov.uk/government/publications/competition-and-markets-authoritys-digital-markets-strategy/the-cmas-digital-markets-strategy-february-2021-refresh>.

<sup>269</sup> EU Commission, "Antitrust: Commission consults stakeholders on a possible new competition tool", press release, 2020, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_977](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_977).



the Commission has identified an imbalance which the market is not able to balance out on its own through competition from competitors because of the dimension of the power imbalance. The answer to the challenge is therefore seen in new rules as existing competition law requires, by virtue of its general rules, a **concrete** analysis of a specific **delineable** market and a finding of **concrete** abusive behaviour by a **specific** undertaking on that market which impairs competition in that segment. The DMA, differing from those rules, considers competition detached from a concrete case by already defining for the online sector (= the specific market) types of behaviour that are to be regarded as abusive if they are applied by predefined actors, the gatekeepers. This replaces lengthy analysis and individual assessment in individual proceedings by the Commission or national authorities and their reactions are swifter. These differences in the approach explain the reliance on Art. 114 TFEU<sup>270</sup>, but at the same time call for a careful consideration of interrelations with other single market-promoting harmonisation rules in sectoral law. This is especially important, as the DMA has obvious connections with for example the Platform-to-Business Regulation,<sup>271</sup> the GDPR<sup>272</sup> or the Audiovisual Media Services Directive<sup>273</sup> to which the DMA is only meant to be complementary but not a substitute when it comes to the digital sector and online platforms.<sup>274</sup>

Following subject matter and general scope (Chapter I), the DMA Proposal contains in Chapter II the conditions under which providers of CPS should be designated as gatekeepers (see more detailed below at 6.3.2). The core section of the DMA Proposal is Chapter III with its list of practices that are assumed to limit competition on the market by reducing contestability and therefore being unfair. It hereby resembles the essential facility doctrine in competition law which requires the holders of facilities that are essential to offer other services and which cannot be replicated to open their facility even to competitors.<sup>275</sup> Monitoring and enforcement of these rules lies at the level of the member states, with the Commission as the central supervisory body. In a remarkable approach, the

---

<sup>270</sup> Schweitzer H. (n 267), p. 6.

<sup>271</sup> Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R1150>.

<sup>272</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (consolidated text), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504>.

<sup>273</sup> Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (codified version), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02010L0013-20181218>.

<sup>274</sup> Cf. on this: de Streel A. and Larouche P., "The European Digital Markets Act proposal: How to improve a regulatory revolution", *Concurrences* 2, 2021, pp. 46-63.

<sup>275</sup> This doctrine has its roots in U.S. law, but is well established in EU competition law and is also especially important in the area of telecommunications and intellectual property, cf. e.g. *Garzaniti et al (ed.), Electronic Communications, Audiovisual Services and the Internet – EU Competition Law & Regulation*, 4th ed. 2020, section 10-294 et seq. See for a recent example on the application of the constitutive *Bronner* case criteria by the CJEU, C-165/19 P – *Slovak Telekom*, para. 38 et seq. (and the parallel case C-152/19 P – *Deutsche Telekom v Commission*, para. 38 et seq.) and the possible implications for application to online platforms Mandrescu D., "Online platforms and the essential facility doctrine – a status update following Slovak Telekom and the DMA", *Lexxion Competition Blog* of 6.4.2021, <https://www.lexxion.eu/en/coreblogpost/online-platforms-and-the-essential-facility-doctrine-a-status-update-following-slovak-telekom-and-the-dma/>.



Commission suggests that neither national authorities nor member states will play a decisive role in the future setup of the supervisory structure (see below 4.). Regarding the concrete powers, Chapter IV provides rules for carrying out market investigations while Chapter V adds rules on the implementation and enforcement of the DMA. The Proposal closes with Chapter VI and general provisions on publication of decisions (Art. 34), a clarification of the unlimited jurisdiction of the Court of Justice of the European Union concerning review of penalties (Art. 35), and the possibility to adopt implementing (Art. 36) and delegated (Art. 37) acts giving the Commission even more powers than those already stemming from the provisions on supervision.

## 6.3. Scope of Application: Broad but few

### 6.3.1. Actors addressed

As the DMA – coupled with the DSA – is aimed at organising the “digital space” in the EU for the coming decades<sup>276</sup>, it is essential that the personal scope covers all those services for which risks have been identified and which the DMA would counteract, while all those services not posing such risks are clearly excluded. The personal scope of the DMA is in a sense twofold: First, CPS are addressed, which are exhaustively listed in Art. 2(2) and defined; second, however, these CPS are only affected by the obligations if they are offered by a provider that has gatekeeper status in this segment, determined by a designation procedure.

#### 6.3.1.1. Core platform Services

The list of CPS in Art. 2(2) covers online intermediation services, online search engines, online social networking services, video-sharing platform services (VSP), number-independent interpersonal communication services, operating systems, cloud computing services and advertising services. At first view, this exhaustive enumeration may be perceived as a limiting factor in terms of an approach that is open to responding to further technological and market developments in the future. However, the proposal refers to the possibility of reconsideration of the list in case future developments indicate that there is a change in a given sector that replicates the same risks as for the currently foreseen services; Art. 17 and Art. 38(2) in that sense in a merely declaratory manner explain that as a consequence of (optional) market investigations or (regular) evaluations of the Regulation new legislative proposals (in this case for amending the list of CPS) can be made.<sup>277</sup> Furthermore the eight types of services already cover a wide range of services and are the result of an evaluation process aimed at identifying services offered in such a way by

---

<sup>276</sup> Cf. Commissioner Thierry Breton according to the Commission press release, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_2347](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347).

<sup>277</sup> Cf. on this *de Streel et al.*, “The European Proposal for a Digital Markets Act: A First Assessment”, <https://cerre.eu/publications/the-european-proposal-for-a-digital-markets-act-a-first-assessment/>, p. 12.



providers in a gatekeeping position that it is very difficult for other businesses to compete on a comparable basis.<sup>278</sup> The Commission chose these services due to several characteristics: extreme scale economies; very strong network effects; multi-sidedness of their services; a significant degree of dependence of both business users and end-users leading to possible user lock-in effects and absence of multi-homing; vertical integration; data driven advantages.<sup>279</sup>

The very specific characteristics have led to several markets being excluded even though there may be dependencies there, too. From a media perspective, although also an important part of the online environment, the sector of video-on-demand services is deliberately not included in the CPS list, because of the lack of lock-in effects (switching costs for consumers are not substantial) and the existence of competition despite a market concentrated on a few providers such as Netflix and Disney+.<sup>280</sup> Limiting the scope of application via precise indications already in the legislative act is important as the consequences attached to applicability of the DMA proposal amount to a significant impact on the rights of the companies concerned.<sup>281</sup>

With regard to the addressed CPS, traditional providers of audiovisual media in the sense of the AVMSD will regularly not themselves fall within the scope of the DMA. However, even if they also operate at least one such CPS, it is unlikely that they will fulfil the gatekeeper criteria (see below at 6.3.1.2). Rather, the relevance for the audiovisual sector stems from the fact that audiovisual media service providers rely or even need to rely on the addressed services in order to be accessible and visible in the digital environment. This is an aspect that is addressed in a very general manner also in the new provision in Art.7a AVMSD with its possibility for member states to introduce measures aimed at ensuring prominence in the dissemination context of audiovisual media services that are of general interest. Concerning the infrastructure for distribution in the list of CPS in particular online intermediation services, online search engines and VSPs are of relevance. These are not defined in the DMA proposal itself, but the list refers to the corresponding definitions in the P2B regulation and the AVMSD thereby enabling a dynamic adjustment in the sectoral laws with effect also for the planned DMA.

Art. 2 of the P2B Regulation defines in point 2 “online intermediation services” as information society services offered on a contractual basis to business users so they may offer goods or services to consumers, with a view to facilitating such initiation of direct transactions between them and the consumers, which at first view appears to have the potential to serve as a kind of catch-all provision for those online services that are not specifically addressed but are already regarded as being offered in potentially problematic market circumstances. Although such an understanding would allow for more flexibility in the DMA, it would also bear the risk of expanding the DMA scope in an unintended way.<sup>282</sup>

---

<sup>278</sup> Cf. *Cole* (n 264), p. 22.

<sup>279</sup> DMA Proposal Recital 2. Cf. for an extensive explanation the Impact Assessment accompanying the DMA proposal, SWD(2020 363) final, Part. 1/2, para 128-130.

<sup>280</sup> On this matter cf. generally the discussion in the EAO Webinar on the Digital Services Act Package, “Gatekeepers in the DSA Package: What about VoD?”, <https://www.youtube.com/watch?v=hlhMwtYQjnU>, minute 22 et seq.

<sup>281</sup> Cf. *Cole* (n 264), p. 25.

<sup>282</sup> Cf. *Cole* (n 264), p. 22 et seq.



Besides that, it is questionable whether this category can really serve to include other services that have an intermediary function and have a key position in the digital environment because of the requirement of a contractual relationship. This criterion leaves the actual significance of this category for the audiovisual sector, for which web browsers or voice assistants could be particularly relevant as key intermediaries, somewhat open.

In also listing VSPs, the DMA addresses a service already included in the new provisions of the revised AVMSD of 2018. While in the AVMSD only a limited number of substantive rules apply to them in comparison to the more extensive framework for audiovisual media service providers, a gatekeeper VSP will have to comply with (additional) obligations under the DMA. In addition to these above-mentioned three particularly important services, further ones that are relevant to the audiovisual sector are included in the list. This is due to the complexity of the digital environment, which offers different channels for distributing and financing the same type of content. For instance, “operating systems” include device-operating software and thereby interfaces of consumers concerning their hardware or software applications, such as for example connected TV devices or app stores and pre-installed software on devices. Also, advertising services are obviously particularly important for the financing of audiovisual media services, at least when it comes to ad-based revenue models which can be affected by business models of platforms, which often do not allow the integration of third-party advertising services and therefore require the business users to rely on the intermediaries’ proprietary advertising services. As the Explanatory Memorandum puts it clearly, this definition is intended to include advertising services that are “related” to one of the other CPS, that is to say it also applies to outsourced services.

#### 6.3.1.2. Gatekeepers and gatekeeper criteria

The notion of gatekeeping has a history that is related to the media sector, although its use as a core concept of the DMA proposal is not an attempt to regulate the media sector specifically. It was discussed already at the beginning of the 20<sup>th</sup> century as a process by which media filter news or rather the news process in a certain way by including or excluding topics, and which results in a kind of bottleneck procedure. Later, bottlenecks were identified in the distribution infrastructure through which media content was delivered to the end user, for example via cable networks. Today’s discussion about gatekeeping is not about news media gatekeeping information but rather intermediaries gatekeeping the media and their content. In a way, the base of the bottle has been widened and the bottleneck shifted and narrowed. However, the DMA does not address the media sector in particular but rather the entire digital sector where “gatekeepers” form an essential link in the relationship between business users and end-users (business-to-consumer [B2C]), but also themselves maintain legal relationships with business users (platform-to-business [P2B]) and end-users (platform-to-consumer [P2C]) and act as an infrastructure for competition between different business users (business-to-business [B2B]). However, a competitive relationship can also exist between platforms and business users if the platform offers its own similar products and services (possibly through affiliated companies). All of these relationships can be affected in a problematic way if the platform reaches a certain size or market power. This describes the systemic relevance – a term which is actually used in the DSA but is indeed the underlying concept of the DMA – of the



gatekeeper in the B2C relationship that the DMA addresses and which necessitates (and justifies) the enactment of special rules for these providers.

In order to only encompass players with a systemic relevance, the DMA uses the gatekeeper criteria listed in Art. 3(1)(a) DMA. A CPS provider has to meet three criteria to be designated as a gatekeeper:

- a) it has a significant impact on the internal market
- b) it operates a core platform service which serves as an important gateway for business users to reach end users
- c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future.

Paragraph 2 then sets thresholds for each of these criteria which, if the CPS exceeds them all, result in the CPS being assessed as a gatekeeper in any case. It is then subject to a notification obligation to the Commission within three months (para 3) as the status of significance, importance and strong position is evident. A significant impact on the market is presumed if the undertaking to which the CPS provider belongs achieves an annual EEA turnover equal to or above EUR 6.5 billion in the last three financial years, or where the average market capitalisation or the equivalent market value of the undertaking to which it belongs amounted to at least EUR 65 billion in the last financial year, and if it provides a core platform service in at least three member states. The gateway criteria are presumed to have been satisfied if the CPS provides a core platform service that has more than 45 million monthly active end-users established or located in the Union and more than 10,000 yearly active business users established in the Union in the last financial year. Finally, the entrenched and durable position is interrelated with the latter criteria and therefore presumed if the user thresholds were met in each of the last three financial years.

Two observations must be made in this context: First, the thresholds are quite high, so that only a few, particularly large and significant players will be covered by the strict rules of the DMA. Therefore, it is to be expected that in practice it will not come down to the details of the criteria. In its impact assessment, the Commission assumes that 10 to 15 providers will be covered by the DMA.<sup>283</sup> This will obviously include the “GAFAM” (Google, Amazon, Facebook, Apple, and Microsoft), which highlights the significance for the media sector as the services provided by the GAFAM (esp. search engines, app stores, ad services) are important channels for the audiovisual industry. Beyond that, the outcome is not yet clearly foreseeable. Large Chinese platforms might not (yet) have a sufficient foothold in the EU market to match the criteria, and smaller platforms that are gatekeepers in niche markets might not meet the thresholds regarding the required number of users.<sup>284</sup> But a few more CPS providers could meet these criteria.<sup>285</sup> Second, the thresholds have to be reached

---

<sup>283</sup> DMA Impact Assessment, SWD(2020) 363 final, part 1, para 148.

<sup>284</sup> Cabral et al, “The EU Digital Markets Act - A Report from a Panel of Economic Experts”, 2021, ISBN 978-92-76-29788-8, doi:10.2760/139337, JRC122910, p. 9.

<sup>285</sup> According to an initial estimate by Caffarra C. and Morton F.C. (The European Commission Digital Markets Act: A translation, 5<sup>th</sup> January 2021, <https://voxeu.org/article/european-commission-digital-markets-act-translation>) Oracle and SAP, for instance, would appear to meet the thresholds, as would AWS and Microsoft Azure. Conversely, in their assessment, Twitter, AirBnB, Bing, LinkedIn, Xbox Netflix, Zoom and Expedia do not



over a certain period of time, which means that CPS providers also have to establish themselves as gatekeepers on the market for a certain duration, which excludes start-ups that achieve a high level of success "overnight". It should nonetheless be pointed out that the gatekeeper designation only concerns the specific CPS of the platform provider which meets the criteria and does not apply to all the CPSs or other services a platform provides.<sup>286</sup>

However, even if a CPS provider does not meet the thresholds or does not meet all of them, it may still be designated as a gatekeeper if the Commission concludes, after a comprehensive assessment, that the criteria in paragraph 1 are nevertheless all met (Art. 3(4)). The criteria to be taken into account in this assessment include, for example, the size, including turnover and market capitalisation, number of business and end-users, entry barriers derived from network effects and data-driven advantages as well as lock-in effects. This is then a more qualitative than purely quantitative assessment which makes the outcome in a specific case less predictable, both from the perspective of potential addressees and the business users and competitors.

### 6.3.2. Designation procedure

The designation procedure first depends on whether a CPS provider meets the thresholds. As mentioned above in that case it has a notification obligation and a duty to provide the Commission with information concerning the thresholds, which must be fulfilled within three months of reaching the thresholds.<sup>287</sup> The Commission then examines this without undue delay, at the latest within a maximum of 60 days, and designates the CPS as a gatekeeper. However, there is a possibility for providers to challenge the (possible) designation in advance and irrespective of the fact that the thresholds of Article 3(2) are actually met. In such a case the Commission has to launch a market investigation, but the providers have to supply the necessary information. The timeline foreseen for this procedure to find out whether or not a designation should take place based on fulfilment of the qualitative criteria is only indicative (five months, according to Art. 15(3) in conjunction with Art. 3(4) and (6)). The procedure which includes a "regulatory dialogue" between the regulator and the regulated can therefore lead to significant time delays (around 10 months) until adoption of measures, even if it is obvious that the concerned provider qualifies as a gatekeeper that meets the thresholds. This delay is exacerbated by the fact that the gatekeeper then has another 6 months to establish compliance with the obligations (Art. 3(8)).<sup>288</sup>

In the case of non-fulfilment of the thresholds, the qualification of a CPS provider as gatekeeper depends on a designation procedure that is initiated via a market

---

appear to meet the thresholds at present, and Booking.com, Spotify, Uber, Bytedance/TikTok, Salesforce, Google Cloud and IBM Cloud appear to meet some but not others at this point.

<sup>286</sup> With reference to Art. 3 para. 7 and Recital 29, de Streel A. et al. (n 277), p. 13.

<sup>287</sup> The DMA Proposal foresees that the Regulation only applies six months after entry into force (Art. 39(2)), but that the designation procedure (as well as further powers of the Commission) shall apply immediately after, which is aimed at speeding up the identification of the main "targets" of the DMA.

<sup>288</sup> In detail on this aspect *Cole* (n 264), p. 26.

investigation carried out by the Commission. If the Commission does not become active on its own behalf, member states can request such an investigation.

In any case, once a gatekeeper is identified, the Commission concludes the procedure by including the gatekeeper in a list. Here, the Commission shall also identify the relevant undertaking to which it belongs and list the relevant core platform services that are provided by that same undertaking and which individually serve as an important gateway for business users to reach end-users as referred to in paragraph 1(b). This leads to legal certainty especially for business customers worldwide but also serves as a signal that specific attention is given to these providers and services.

## 6.4. Obligations and Prohibitions or ‘Do’s and don’ts’ for Gatekeepers

Art. 5-7 of the DMA proposal contain a number of very specific obligations gatekeepers have to comply with concerning partly the behaviour towards business users of the gatekeeper services and partly the rights that end-users including customers of the business users of the gatekeeper services are being given. They can be categorised according to which problems they tackle: addressing a lack of transparency in the (advertising) market; preventing platform envelopment;<sup>289</sup> facilitating the mobility of business users and clients; preventing practices that are unfair.<sup>290</sup>

### 6.4.1. Structural aspects

Regarding the structure of the obligations, reference was and often still is made, in the discussion, to a black, a grey and a whitelist. This can be traced back to a list of “unfair practices” in a preparatory document of the Commission that was leaked and comprised a blacklist and a grey list, but also referred to a whitelist to be established. As the final proposal does not use this terminology<sup>291</sup> or structure, it is preferable to refrain from using these terms and address the provisions of Art. 5 and 6 DMA Proposal as what they are: obligations for gatekeepers which list certain ‘do’s and don’ts’ in terms of their business practices. However, the distinction between the obligations laid down in Art 5 and 6 needs to be taken into account and should be clarified before taking a closer look at some of the obligations which are of particular relevance for the (audiovisual) media sector.

---

<sup>289</sup> Envelopment in this regard refers to one platform provider moving into the (not necessarily related) market of another platform or provider of services where comparable user groups exist; by combining its own functionalities with the new ones of the target market it can prompt a foreclosure of the second market: its users are addressed in an exclusive manner and are oriented away from the incumbent platform.

<sup>290</sup> This categorisation was proposed by de Streel et al. (n 277), p. 19.

<sup>291</sup> Cf. on possible reasons Georgieva Z., “The Digital Markets Act Proposal, of the European Commission: Ex-ante Regulation, Infused with Competition Principles”, <https://www.europeanpapers.eu/fr/europeanforum/digital-markets-act-proposal-european-commission-exante-regulation>.



Article 5 contains “obligations for gatekeepers” while Art. 6 refers to “obligations for gatekeepers susceptible of being further specified”. Irrespective of the concrete nature of the obligations contained therein, Art. 7(1) underlines that measures implemented by the gatekeeper to ensure compliance shall be effective in achieving the objective of the relevant obligation in both provisions. Art. 5 and 6 are also treated in the same way with regard to a possible suspension of the obligations which gatekeepers can request exceptionally (Art. 8), the updating of the rules through delegated acts (Art. 10), the prohibition of circumvention (Art. 11) as well as for the Commission’s enforcement powers, as can be seen with the market investigation procedure (Art. 15 and 16) and the monitoring (in particular Art. 22 to 25) and sanctioning measures (Art. 26 and 27). Although both provisions are binding directly, that is to say they must be fulfilled after the six-month period following the designation and sanctions can be levied in case of non-compliance, the difference is that with regard to the obligations in Art. 6 the Commission is empowered to adopt implementing acts for some of the obligations according to Art. 36 DMA Proposal and has the possibility to lay down, in a specific decision directed at a gatekeeper, the way in which an obligation needs to be achieved. Recitals 29 and 33, but also Recital 58, suggest here a procedure involving the gatekeepers in defining such measures through a “regulatory dialogue” which is intended to “facilitate compliance by gatekeepers and expedite the correct implementation of the Regulation”. However, the DMA itself lacks clarity when it comes to the role of the gatekeepers in this “dialogue” as well as the procedure under which it takes place. One can already question the need for such a procedure, as, after all, Art. 6 specifications are already the result of a case-by-case assessment of the Commission that the measures implemented (or possibly foreseen) by the given provider are likely not sufficient. The distinction seems motivated by the idea that for some obligations the measures to be taken might depend on the actual gatekeeper (and the specific service offered by it) and may be different in comparison to others or that the obligation’s consequences are not as self-explanatory or obvious as for the obligations under Art. 5. At the same time, this additional layer of intervention may in practice lead to a delayed enforcement and therefore it should be carefully weighed in the forthcoming legislative process regarding whether or not an obligation is listed in Art. 5 or 6 DMA or whether they can be merged completely and the flexibility of the Commission ensured in other ways.

Apart from this, the individual obligations within the provisions do not follow any particular order.<sup>292</sup> In both provisions the obligations are either formulated as duties to act (allow, provide) or duties to refrain from a specific behaviour. However, that does not mean that the obligations to refrain are limited to abstaining from a certain action, as for some of the concerned provisions active measures might be necessary to reach the level of compliance required by the obligation itself and the further details in the respective recitals, for most of the obligations. Furthermore, for both provisions the DMA proposal includes possibilities for concretising the obligations through delegated acts (Art. 37, concerning Art. 5 and 6) and the adoption of implementing provisions (Art. 36, concerning Art. 6). This aims at keeping the list of obligations up-to-date in responding to practices that may only surface in the future but have a negative impact on the market equivalent to the ones already included.

---

<sup>292</sup> Cf. on this with alternative proposals for listing, Monti G., “The Digital Markets Act – Institutional Design and Suggestions for Improvement”, TILEC Discussion Paper 2021-004, p. 3.

The Commission has the possibility to suspend a CPS from the obligation wholly or partly for a certain period of time (Art. 8) and/or to exempt a gatekeeper from a specific obligation for overriding reasons of public interest including morality, health and security issues (Art. 9).

## 6.4.2. Close-up on some of the obligations

To create a fair and contestable market, the DMA proposes a wide set of different obligations approaching this goal from different angles. In particular, gatekeepers should refrain from merging personal data from the core services with data from other services. The gatekeepers may not prevent their business customers from complaining to supervisory authorities. Gatekeepers shall no longer prevent users from uninstalling pre-installed software or apps or from accessing services they may have purchased outside the gatekeeper platform. Gatekeepers shall not use data obtained from their business users to compete with those business users. They should also not be allowed to make the use of their services conditional on registration with another of their services. On the other hand, they must allow business customers to offer their services and products also through third-party intermediary services at different prices and to advertise their offers and conclude contracts with their customers outside the gatekeeper's platform. Gatekeepers must provide businesses advertising on their platform with access to the gatekeeper's performance measurement tools and to the information (e.g. on prices) necessary to enable advertisers and publishers to conduct their own independent review of their advertising portfolio on the gatekeeper service. This includes data generated by the business customers' use of the platform. In addition, specific situations are defined in which gatekeepers must allow third parties to interact with the gatekeeper's own services, in other words to ensure interoperability. Looking at these different obligations it becomes clear that several are of high relevance for audiovisual media service providers from the perspective of a competitor of the gatekeeper as well as from the point of view of a business user relying on the gatekeeper's services.

Especially online advertising is an essential element for the refinancing of content production and is therefore directly relevant for media pluralism, and has been very opaque in the past. Google and Facebook, constituting a "quasi-duopoly" in search and display advertising<sup>293</sup> are the gatekeepers in this area which cannot be bypassed by business users. Although there are different business models in audiovisual media – besides advertising, revenue-based free-to-air services, also subscription-based refinancing models – and therefore some of the obligations applicable to gatekeepers are of greater relevance depending on the model, the advertising information is crucial for all. The relevant provisions of the DMA proposal in this regard are Art. 5(g) and 6(1)(g), both concerning access to information about the functioning of online advertising value chains and therefore aiming to ensure transparency and a balancing of the prevailing information imbalance in the advertising market. Art. 5(g) obligates gatekeepers to provide advertisers and publishers

---

<sup>293</sup> UK Competition and Markets Authority (CMA) "Online platforms and digital advertising market study", 2020, <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study>.



to which they supply advertising services, with information concerning the price paid by the advertiser and publisher, as well as the amount or remuneration paid to the publisher, for the publishing of a given ad and for each of the relevant advertising services provided by the gatekeeper, upon their request. Recital 42 points out that the information only has to be provided “to the extent possible” taking into account the high complexity of the advertising value chain.<sup>294</sup> Art. 6(1)(g) adds to this, transparency about how the advertising performs by giving business users access to the performance-measuring tools of the CPS (or an advertising agency relied on, according to Recital 53), which is meant to enable them to decide about possible changes they would like to make in order to improve efficiency. These obligations deliver crucial instruments to tackle the existing information imbalance in the field of programmatic advertising that media services are confronted with.

Another imbalance relevant to the media sector is addressed by Art. 5(a) and 6(1)(a), namely that of power over large amounts of data. The parallel signing in to several services and using the “entrance door” of a user account to one CPS in order to facilitate the use of other services, thereby giving such companies access to a wide range of data of their users, has put other service providers in a disadvantaged position.<sup>295</sup> The issue of data accumulation has therefore been intensely discussed from the perspective of data protection law, but it has also been picked up by competition authorities because of the implications for competitors and end-users.<sup>296</sup> The DMA has now reacted to an urgent need for clarification of abusive practices in data accumulation as identified by several competition authorities of the member states with prohibitions inserted into a Regulation creating EU-wide consistency once in force. Art. 5(a) obligates gatekeepers to refrain from combining personal data sourced from the CPS with personal data from any other services offered by the gatekeeper or by third parties without the freely given consent of the user. Art. 6(1)(a) takes into account more the business user perspective by prohibiting gatekeepers from using, in competition with business users, any data not publicly available which is generated through activities by those business users, including by the end-users of these business users, that is to say ensuring that business users cannot be locked out from using their own data.

Finally, it is also worth taking a brief look at the provisions aiming to counteract the imbalance created by lock-in-effects on platforms which can also present an issue for pluralism. Art. 6(1)(h) introduces a data portability obligation that requires gatekeepers to allow business and end-users to “take their data” with them when switching to other service providers offering comparable services for which the (already created) data continues to be of relevance. Going beyond the obligation from data protection law to ensure data portability (Art. 20 GDPR), portability shall be facilitated by “continuous and real-time access” to the data for both business and end-users. A similar obligation, also in technical terms as it relates again to “effective, high-quality, continuous and real-time access”, follows from Art. 6(1)(i) which obligates the gatekeeper to provide business users free of charge with aggregated or non-aggregated data that is provided for or generated in the

---

<sup>294</sup> Cf. on this Knapp D., “Media pluralism from an economic perspective: Algorithmic media – new considerations for media plurality”, in: Cappello M. (ed.), *Media pluralism and competition issues*, IRIS Special, European Audiovisual Observatory, Strasbourg 2020, p. 9, 16.

<sup>295</sup> In more detail Cole M.D.(n 264), p. 30 et seq.

<sup>296</sup> *Etteldorf* (n 263), p. 243 et seq.



context of the use of the relevant CPS by those business users and the end-users engaging with the products or services provided by those business users. However, the limits of the GDPR must be respected if this concerns personal data, in other words the end-user retains the right of disposition, so that his or her consent may be required. This clearly enhances the competitive position of business users of platforms vis-à-vis the platforms and improves return-on-investment possibilities. Art. 5(f) complements the counteracting of lock-in effects by preventing their intensification: Gatekeepers are prohibited from requiring business users or end-users to subscribe to or register with any CPS.

Overall, the provisions help to create at least the appropriate infrastructure for an online environment that allows for diversity in which users can choose from a variety of services without major obstacles.

## 6.5. Enforcement: A centralised approach

With regard to supervision and enforcement of the proposed Regulation, the DMA follows a centralised approach with the European Commission being the core actor. In that sense it differs from the DSA.<sup>297</sup> To ensure the appropriate and up-to-date adoption of the rules, the DMA Proposal entrusts the Commission on the one hand with several powers to carry out market investigations (Art. 15-17), in particular for the designation of a core platform service as a gatekeeper, investigations of systematic non-compliance and of new core platform services and new practices, as well as with regulatory and enforcement powers. The powers include requesting information, conducting interviews, on-site inspections at the investigatory stage, adoption of interim measures, making binding commitments of the gatekeeper, monitoring, and finally issuing non-compliance decisions as well as imposing fines or periodic penalty payments under certain conditions. With these powers the Commission performs the central function of supervision for the DMA.

The member state authorities, to the contrary, do not play a role in the setup. And for the member states themselves, the usual committee accompanying Regulations that empower the Commission to pass delegated acts is created as a Digital Markets Advisory Committee in following the rules laid down in Regulation (EU) No 182/2011<sup>298</sup>. It is composed of representatives of member states and shall give opinions on certain individual decisions of the Commission, but it is not equipped with regulatory powers. Besides that, the DMA Proposal provides for a possibility for three or more member states to request the Commission to open a market investigation pursuant to regarding the designation of (new) gatekeepers (Art. 33).

It should be recalled that the DMA proposal leaves competition law instruments untouched, and thereby national authorities retain the power to apply national competition

---

<sup>297</sup> On the setup under the DSA proposal cf. Cole M D., Etteldorf C., Ullrich C., “Updating the Rules for Online Content Dissemination” (n 259), p. 202 et seq.

<sup>298</sup> Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission’s exercise of implementing powers, OJ L 55, 28.2.2011, p. 13–18, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32011R0182>.



law to these providers independently of the rules of the DMA. However, it is not clear whether contradicting results are possible and how these would be resolved considering that the DMA would be a later rule compared to the established competition law regime.<sup>299</sup> Moreover, besides competition law, national rules, in particular those serving public interests such as safeguarding media pluralism (cf. Art. 1(5) DMA proposal), remain applicable and enforceable.

This centralised approach resembles what is known for example from the EU Merger Regulation or the Single Supervisory Mechanism for banking supervision.<sup>300</sup> The international dimension of the problem triggering the DMA proposal and the fact that it is a Regulation makes such a centralised approach appear to be the obvious type of approach. However, both the DSA proposal and the GDPR are examples of the fact that the Regulation does not necessarily speak in favour of centralised supervision. The Commission's argument here is that only a few big players are addressed and they operate their services across the EU, so it makes sense to assign them to a single regulator as the point of contact. The regulatory dialogue, which is envisaged in some places as shown, is easier to implement than if it were coordinated by several national authorities. Even though each of them is different in nature, the possibility of a joint approach by all member states' competent authorities can be coordinated, for example by the European Data Protection Board or the European Regulators Group for Audiovisual Media Services. Some authors argue with economic and financial aspects: monitoring compliance is likely to be costly and may require careful large-scale data analysis or direct review of algorithm design where it would be highly unlikely that individual national regulators would be well set up to do this.<sup>301</sup> The Directorate General for Competition already implements the EU competition rules in merger control and antitrust proceedings and "overall [...] made good use of its enforcement powers", as the European Court of Auditors recently stated in a special report, while also noting that "improvements are necessary in a number of areas".<sup>302</sup> However, as described repeatedly above, the DMA is not an instrument of competition law. Whether set up on a national level or by the Commission on the EU level, a new unit would have to be created and provided with resources. Coordination with national authorities, in particular competition and data protection authorities, will therefore be necessary at least because of overlaps of the DMA with these areas and the requirement for a necessary degree of consistency and coherence and, more generally speaking, in order to ensure a coordinated approach in the platform environment.<sup>303</sup>

---

<sup>299</sup> Fernández C., "A New Kid on the Block: How Will Competition Law Get along with the DMA?", *Journal of European Competition Law & Practice*, 12(4), 2021, pp. 271-272, argues for the need for extensive coordination and improvement of the DMA proposal in this respect. A differing view is presented by Schweitzer H.(n 267), p. 13.

<sup>300</sup> Cf. on this Monti G. (n 292), p. 4 et seq.

<sup>301</sup> Monti G. (n 292), p. 5.

<sup>302</sup> "The Commission's EU merger control and antitrust proceedings: A need to scale up market oversight", report 24/2020, [https://www.eca.europa.eu/Lists/ECADocuments/SR20\\_24/SR\\_Competition\\_policy\\_EN.pdf](https://www.eca.europa.eu/Lists/ECADocuments/SR20_24/SR_Competition_policy_EN.pdf).

<sup>303</sup> Georgieva Z.(n 291).

## 6.6. Conclusion

The DMA proposal is an ambitious, likely necessary and much-awaited instrument to regain more control of the platform market with its unprecedented concentration and market power of a few players due to unusual network effects. Obviously, as it enables significant interference with prevailing business models of these providers which in future would qualify as gatekeepers, it is likely that in the further legislative procedure there will be lengthy controversial discussions. Leaving aside the discussion about the appropriateness of the individual elements of the DMA proposal, a very important aspect to take carefully into consideration is the need to integrate all elements of the Digital Services Act Package with existing instruments on the EU and national level.

The DMA has the potential to serve as an instrument filling in the missing pieces in the regulatory framework when it comes to the specifics of the largest online platforms and the crucial nature of services offered by them which are conditional for other providers being able to offer services to end-users. It will be a more powerful, certainly faster and more flexible – as it applies *ex ante* before a market failure appears or is cemented and without the need to prove the unfair market behaviour in a specific case – instrument than existing competition law, but again there should be a discussion whether procedures can be aligned with this area of existing experience in cooperation with and between the national authorities and the Commission.

The DMA proposal is most noteworthy for the fact that it clearly states that the European Union is not willing to leave issues in the most relevant markets for businesses and citizens alike in our digital world unaddressed. And that it will do so based on values and principles on which the EU – and its member states – are built. In doing so, there is potential for the DMA to be yet another “gold standard” of platform regulation – as was the case with the GDPR – with an impact across the world once it is in place and applied properly within the EU.



### ***A matter of scope?***

*Usual readers of our publications may be puzzled at one important fact: while the scope of both the DMA and DSA includes video-sharing platforms such as YouTube and the like, it excludes video-on-demand (VoD) platforms such as Netflix, Amazon Prime or Disney+. VoD providers remain subject to the obligations of the Audiovisual media services directive, as they imply editorial responsibility, an element lacking in the case of intermediaries, to which the DSA applies.*

*And yet, the notion of gatekeeping may seem akin to the position of certain players in the VoD arena. Some of our readers might indeed ask themselves the following question: should the DMA include in its scope VoD services?*

***Oliver Budzinski** focuses in the following chapter on the economics of gatekeeping in the audiovisual sector and provides his insights about problems and possible solutions.*



# 7. Gatekeeping in the audiovisual sector: economic background, competition, and regulation

*Oliver Budzinski, Ilmenau University of Technology\**

## 7.1. Introduction

In the context of the current initiative of the European Union to regulate online services with the proposed Digital Services Act package (“DSA package”),<sup>304</sup> the term “gatekeeper” has risen to new prominence. It is both emphasized in the Digital Markets Act proposal and – subsequently – in the academic literature discussing the proposals for regulating big tech companies.<sup>305</sup> Any regulation of business activities in markets is always subject to both economic and legal reasoning. Economics aims to identify (i) conditions under which

---

\* Professor of Economic Theory, Director of the Institute of Economics, Institute of Media and Mobile Communication, Ilmenau University of Technology, Germany, Email: [oliver.budzinski@tu-ilmenau.de](mailto:oliver.budzinski@tu-ilmenau.de). I thank Sophia Gaenssle, Maja Cappello and Francisco Cabrera for valuable comments on an earlier draft of this paper.

<sup>304</sup> The Digital Services Act package contains two legislative initiatives to upgrade rules governing digital services in the EU: the Digital Services Act (DSA) and the Digital Markets Act (DMA). See Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN>; and Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), COM/2020/842 final, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN>.

<sup>305</sup> See also the discussion in Chapter 6 of this publication. For the – economic and legal – academic debate on the DSA/DMA-package see, inter alia, Cabral, L. et al., “The Digital Markets Act: A Report from a Panel of Economic Experts”, Luxembourg: European Union 2021, <http://dx.doi.org/10.2760/139337>; Bentata, P., “Regulating Gatekeepers: Predictable Unintended Consequences of the DMA for Users’ Welfare”, 2021, <https://ssrn.com/abstract=3804067>; Podszun, R., Bongartz, P. and Langenstein, S., “Proposals on how to Improve the Digital Markets Act”, Policy paper in preparation for the information session on the Digital Markets Act in the European Parliament’s Committee on Internal Market and Consumer Protection (IMCO) on 19 February 2021, <https://ssrn.com/abstract=3788571>; Vezzoso, S., “The Dawn of Pro-Competition Data Regulation for Gatekeepers in the EU”, 2021, <https://ssrn.com/abstract=3772724>; Geradin, D., “What Is a Digital Gatekeeper? Which Platforms Should Be Captured by the EC Proposal for a Digital Markets Act?”, 2021, <https://ssrn.com/abstract=3788152>; Leistner, M., “The Commission’s Vision for Europe’s Digital Future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act – A Critical Primer”, 2021, <https://ssrn.com/abstract=3789041>; De Streef, A. et al., “The European Proposal for a Digital Markets Act: A First Assessment”, Cerre 2021; <https://cerre.eu/publications/the-european-proposal-for-a-digital-markets-act-a-first-assessment/>; Kerber, W., “Taming Tech Giants With a Per-Se Rules Approach? The Digital Markets Act from the ‘Rules vs. Standard’ Perspective”, *Concurrences*, 2021, forthcoming.



incentives to gatekeeping behaviour are generated, and (ii) effects of gatekeeping on consumer and social welfare. Legal science deals with (i) the codification of rules for markets affected by gatekeeping and for gatekeepers (companies) in law and (ii) the enforcement of these rules. In a sound regulatory system, the law represents the underlying economics in the sense that welfare-reducing business strategies are frustrated by the law (and, thus, indirectly welfare-increasing ones promoted). Consequently, regulating gatekeeping needs to embrace the economics of gatekeeping for the sake of social welfare.

This contribution focuses on the economics of gatekeeping in the audiovisual sector. Audiovisual content is increasingly consumed online with younger generations already using predominantly online services whereas older generations still focus more on traditional channels (traditional television as free-to-air, cable, or satellite television). The movement away from traditional television towards online services can be observed in virtually all age groups, although to different extents.<sup>306</sup> Online services in the audiovisual sector include the Internet-based broadcast of traditional television as well as new types of services like on-demand audiovisual media services<sup>307</sup> (e.g. Netflix, AmazonPrime, Disney+, DAZN, HBO Max, etc.) and marketplace-style video-sharing platforms<sup>308</sup> (e.g. YouTube, TikTok, Facebook, Dailymotion, etc.).<sup>309</sup> A major difference between traditional television that is “just” broadcast online and most purpose-built online streaming services is the linearity of the programme: while traditional television provides programmes with fixed time slots, most streaming services offer non-linear video on demand, that is to say

---

<sup>306</sup> See for a review and summary of recent developments in Germany Lindstädt-Dreusicke, N. and Budzinski, O., “The Video-on-demand Market in Germany – Dynamics, Market Structure and the (Special) Role of YouTube”, *Journal of Media Management and Entrepreneurship* 2(1), 2020, 108-123,

<http://dx.doi.org/10.4018/JMME.2020010107>, and more generally Budzinski, O., Gaenssle, S. and Lindstädt-Dreusicke, N., “The Battle of YouTube, TV and Netflix – An Empirical Analysis of Competition in Audio-visual Media Markets”, *Ilmenau Economics Discussion Papers* 26(137), 2020, <http://dx.doi.org/10.2139/ssrn.3569553>.

<sup>307</sup> According to Article 1(1)(g) of the Audiovisual Media Services Directive (AVMSD), “on-demand audiovisual media service’ (i.e. a non-linear audiovisual media service) means an audiovisual media service provided by a media service provider for the viewing of programmes at the moment chosen by the user and at his individual request on the basis of a catalogue of programmes selected by the media service provider”. See Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (codified version) (Text with EEA relevance), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02010L0013-20181218>.

<sup>308</sup> According to Article 1(1)(aa) AVMSD, “video-sharing platform service’ means a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing”.

<sup>309</sup> For categorisations of business model types see, inter alia, Lindstädt-Dreusicke, N. and Budzinski, O., “The Video-on-demand Market in Germany – Dynamics, Market Structure and the (Special) Role of YouTube”, *Journal of Media Management and Entrepreneurship* 2(1), 2020, 108-123, <http://dx.doi.org/10.4018/JMME.2020010107>. Note that business models develop and mixed models as well as model innovations are possible; business models may also converge in the future, rendering classifications obsolete. The same is true for the alternative classification in retail-style video broadcasting and marketplace-style video sharing services.



consumers can decide when to watch what content.<sup>310</sup> Recent research shows that linear television and non-linear streaming services compete with each other with both comparable types of content and for at least partly the same consumers (and advertisers if the service is advertising-financed).<sup>311</sup> There has been a controversy about whether video-sharing platforms compete with both traditional television and on-demand audiovisual media services, because they are said to provide markedly different content appealing to different consumers and/or for different consumption purposes.<sup>312</sup> Instead of movies, serials, and features, consumers of video-sharing platform services predominantly watch shorter videos (especially music videos and tutorials), non-commercial content (cat/funny videos, etc.) and commercial content from social media stars (including unboxing videos, lifestyle and beauty content, and video gaming/e-sports).<sup>313</sup> However, recent research indicates that, despite these differences, video-sharing platforms exert relevant competitive pressure on both traditional television and on on-demand audiovisual media services.<sup>314</sup> Therefore, I will not distinguish between submarkets in the audiovisual sector in the following analysis. Instead, I will refer to video streaming services or video-on-demand (VoD) services to cover both video-sharing platforms and on-demand audiovisual media services.

## 7.2. Competition and gatekeepers in the digital economy: The underlying economics

With respect to media markets, gatekeeping has long been associated with predominantly two issues: (i) the power of editorial offices to select what the audience of television, radio and (printed) newspapers gets to view, listen to and read, and (ii) the power of (mostly) government agencies to allocate scarce frequencies for free-to-air radio and television

---

<sup>310</sup> Note that some content types like live broadcasts of sports events will have a fixed time slot in online streaming catalogues as well.

<sup>311</sup> See Prince, J. and Greenstein, S., “Measuring Consumer Preferences for Video Content Provision via Cord-Cutting Behavior”, *Journal of Economics & Management Strategy* 26(2), 2017, 293-317, <https://doi.org/10.1111/jems.12181>; McKenzie, J. et al., “Experimental Evidence on Demand for ‘On-demand’ Entertainment”, *Journal of Economic Behavior and Organization* 161, 2019, 98-113, <https://doi.org/10.1016/j.jebo.2019.03.017>; Budzinski, O., Gaenssle, S. and Lindstädt-Dreusicke, N., “The Battle of YouTube, TV and Netflix – An Empirical Analysis of Competition in Audio-visual Media Markets”, *Ilmenau Economics Discussion Papers* 26(137), 2020, <http://dx.doi.org/10.2139/ssrn.3569553>.

<sup>312</sup> See for a recent summary of the controversy Budzinski, O. and Lindstädt-Dreusicke, N., “Antitrust Policy in Video-on-Demand Markets: The Case of Germany”, *Journal of Antitrust Enforcement* 8(3), 2020, 606-626, <https://doi.org/10.1093/jaenfo/jnaa001>.

<sup>313</sup> See on the commercial and professional character of audiovisual content related to social media stars Budzinski, O. and Gaenssle, S., “The Economics of Social Media (Super-)Stars: An Empirical Investigation of Stardom and Success on YouTube”, *Journal of Media Economics*, 31(3-4), 2020, 75-95, <https://doi.org/10.1080/08997764.2020.1849228>; Gaenssle, S. and Budzinski, O., “Stars in Social Media: New Light Through Old Windows?”, *Journal of Media Business Studies* 18(2), 2021, 79-105, <https://doi.org/10.1080/16522354.2020.1738694>; Gaenssle, S., “Attention Economics of Instagram Stars: #Instafame and Sex Sells?” *Ilmenau Discussion Papers* 27(150), 2021, <http://dx.doi.org/10.2139/ssrn.3861486>.

<sup>314</sup> See Budzinski, O., Gaenssle, S. and Lindstädt-Dreusicke, N., “The Battle of YouTube, TV and Netflix – An Empirical Analysis of Competition in Audio-visual Media Markets”, *Ilmenau Economics Discussion Papers* 26(137), 2020, <http://dx.doi.org/10.2139/ssrn.3569553>.



transmission.<sup>315</sup> Consequently, gatekeeping in this sense refers to the ability to inhibit or advance the flow or circulation of information, so that a specific type of market power results.<sup>316</sup> This market power manifests in the ability to (imperfectly) determine which contents make it through to the potential attention of large audiences and which not, or in other words: “gatekeepers (...) control access to the audience in media markets”.<sup>317</sup> Notably, the above-mentioned two issues of traditional gatekeeping in media markets have to a large extent disappeared in the digital age: the Internet allows everyone to publish their content (at least technically) and digitization has eroded the need for scarce frequencies to reach the audience. This development has fuelled doubt about the relevance of gatekeeping in digital media markets.<sup>318</sup>

By contrast, the empirical picture shows several companies that are clearly gatekeepers in the sense that they effectively control access to the audience, consumers, or other relevant groups of market players.<sup>319</sup>

- Google Search dominates the market for (horizontal) search engines in many markets across the world, often with market shares in excess of 80% and even 90%. Furthermore, the Alphabet-Google group controls significant shares of the business-to-business information flow in the markets for online advertising.<sup>320</sup>
- Everyone who wants to use or sell smartphone apps is de facto forced to use the marketplaces The Apple App Store for Apple devices (100%) and GooglePlay for Android devices (market shares often more than 90%), giving these marketplace

---

<sup>315</sup> See, inter alia, the survey by Heinderyckx, F. and Vos, T., “Reformed Gatekeeping”, *Communication & Media* 11(38), 2016, 29-46, <https://dx.doi.org/10.5937/comman11-10306>.

<sup>316</sup> See Heinderyckx, F. and Vos, T., “Reformed Gatekeeping”, *Communication & Media* 11(38), 2016, 29-46, <https://dx.doi.org/10.5937/comman11-10306>.

<sup>317</sup> Gaenssle, S. and Budzinski, O., “Stars in Social Media: New Light Through Old Windows?”, *Journal of Media Business Studies*, 18(2), 2021, 79-105, p. 90, <https://doi.org/10.1080/16522354.2020.1738694>.

<sup>318</sup> See Heinderyckx, F. and Vos, T., “Reformed Gatekeeping”, *Communication & Media* 11(38), 2016, 29-46, <https://dx.doi.org/10.5937/comman11-10306> as well as Gaenssle, S. and Budzinski, O., “Stars in Social Media: New Light Through Old Windows?”, *Journal of Media Business Studies* 18(2), 2021, 79-105, <https://doi.org/10.1080/16522354.2020.1738694>. While both disagree with the notion of no gatekeeping in digital media markets, they reference the skeptical literature.

<sup>319</sup> See, on the following cases, inter alia, Crémer, J., de Montjoye, Y.A. and Schweitzer, H., *Competition Policy for the Digital Era*, Publications Office of the European Union, Luxembourg, 2019,

<http://dx.doi.org/10.2763/407537>; Marsden, P. and Podszun, R. (2020), *Restoring Balance to Digital Competition – Sensible Rules, Effective Enforcement*. Berlin: Konrad-Adenauer-Stiftung, <https://www.kas.de/documents/252038/7995358/Restoring+Balance+to+Digital+Competition+%E2%80%93+Sensible+Rules+Effective+Enforcement.pdf/7cb5ab1a-a5c2-54f0-3dcd-db6ef7fd9c78?version=1.0&t=1601365173489>;

Bougette, P., Budzinski, O. and Marty, F., “Exploitative Abuse and Abuse of Economic Dependence: What Can We Learn from an Industrial Organization Approach?” *Revue d’Economie Politique* 129(2), 2019, 261-286,

[https://www.cairn-int.info/article.php?ID\\_ARTICLE=E\\_REDP\\_292\\_0261](https://www.cairn-int.info/article.php?ID_ARTICLE=E_REDP_292_0261); Budzinski, O., Grusevaja, M. and Noskova, V., “The Economics of the German Investigation of Facebook’s Data Collection”, *Market and Competition Law Review* 5(1), 2021, 43-80, <https://doi.org/10.34632/mclawreview.2021.10008>.

<sup>320</sup> See European Commission, *Case AT.39740 – Google Shopping*, Brussels 2017, [https://ec.europa.eu/competition/antitrust/cases/dec\\_docs/39740/39740\\_14996\\_3.pdf](https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf).



providers power over (i) the apps that users can use and (ii) the information flow about sales, user response, and other data to the app producers.<sup>321</sup>

- The Facebook group (including also Instagram and WhatsApp) controls to a considerable extent the circulation of information in social network services – although the uprising of TikTok may challenge this position.<sup>322</sup>
- Amazon with its online marketplace controls in particular the information flow to the shops that are present in the marketplace but – based on this information advantage – also which products its retail arm offers and which products are left to the shops in the marketplace. Via its search function and ranking, it also significantly influences what offerings are brought to the attention of the consumers.<sup>323</sup>

The first three examples in this (incomplete and exemplary) list are clearly connected to dominant market positions whereas this is more difficult with Amazon Marketplace due to the ambiguity of determining the relevant market here (do online shops operate in different markets than offline shops if they sell roughly similar goods?). This is well in line with traditional standard economics, which would conclude that effective competition should prevent the accumulation of gatekeeping power. However, the digital age and the peculiar business of online services has also fueled theory development in economics. Three streams of specific digitisation/online business-related theories in particular have emerged:<sup>324</sup>

- Platform economics:<sup>325</sup> Online services may feature platform characteristics which are defined as (i) managing two or more distinct customer groups that (ii) are

---

<sup>321</sup> See Geradin, D. and Katsifis, D., “The Antitrust Case Against the Apple App Store”, TILEC Discussion Paper No. DP2020-039, 2020, <http://dx.doi.org/10.2139/ssrn.3583029>; Marty, F. and Pillot, J., “Cooperation, Dependence, and Eviction: How Platform-to-business Coopetition Relationships Should Be Addressed in Mobile Telephony Ecosystems”, in: D. Bosco and M. Gal (eds.), *Challenges to Assumptions in Competition Law*, Cheltenham: Elgar 2021, 2-22; Budzinski, O., Gaenssle, S. and Lindstädt-Dreusicke, N., “Wettbewerb und Antitrust in Unterhaltungsmärkten”, in: O. Budzinski, J. Haucap, A. Stöhr and D. Wentzel (Eds.), *Zur Ökonomik von Sport, Entertainment und Medien – Schnittstellen und Hintergründe*, Berlin: DeGruyter, 2021, forthcoming.

<sup>322</sup> See Podszun, R., “Regulatory Mishmash? Competition Law, Facebook and Consumer Protection”, *Journal of European Consumer and Market Law* 8(2), 2019, 49-52, <https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/8.2/EuCML2019010>; Buiten, M. C., “Exploitative Abuses in Digital Markets: Between Competition Law and Data Protection Law”, *Journal of Antitrust Enforcement* 9, 2021, <https://doi.org/10.1093/jaenfo/jnaa041>; Budzinski, O., Grusevaja, M. and Noskova, V., “The Economics of the German Investigation of Facebook’s Data Collection”, *Market and Competition Law Review* 5(1), 2021, 43-80, <https://doi.org/10.34632/mclawreview.2021.10008>; Kerber, W. and Zolna, K., *The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law*, 2020, <http://dx.doi.org/10.2139/ssrn.3719098>.

<sup>323</sup> See Budzinski, O. and Köhler, K.H., “Is Amazon The Next Google?” *ORDO*, 66(1), 2015, 263-288; Khan, L.M., “Amazon’s Antitrust Paradox”, *The Yale Law Journal*, 126(3), 2017, 710-805.

<sup>324</sup> See for an overview of the modern industrial economics of media industries Budzinski, O. and Kuchinke, B.A., “Industrial Organization of Media Markets and Competition Policy”, in: M.B. von Rimscha (ed.), *Management and Economics of Communication*, Berlin: DeGruyter 2020, 21-45.

<sup>325</sup> See, inter alia, Armstrong, M., “Competition in Two-sided Markets”, *The RAND Journal of Economics* 37(3), 2006, 668-691; Caillaud, B. and B. Jullien. “Chicken & Egg: Competition among Intermediation Service Providers”, *The RAND Journal of Economics* 34(2), 2003, 309-328.; Evans, D.S. and R. Schmalensee; “The Antitrust Analysis of Multisided Platform Businesses”, in: R.D. Blair and D.D. Sokol (eds.), *The Oxford Handbook of International Antitrust Economics*, Oxford: Oxford University Press 2015, 404-447; Haucap, J. and T. Stühmeier,



interconnected through indirect network effects with (iii) relevant transaction costs hampering a direct self-coordination between the customer groups. Offline as well as online media may appear to have platform characteristics if they are at least partly financed by advertising.<sup>326</sup> Advertising-financed commercial television represents an example where the television company manages the two customer groups' viewers and advertisers. For advertisers, the value of a television broadcast increases with the number of viewers (in total or out of certain target groups), which represents a positive indirect network effect from the customer group viewers to the customer group advertisers.<sup>327</sup> The same is true for advertising-financed online content (like YouTube video streaming). However, in media markets, the platform character is not inherent like it is in the markets where platform economics was originally applied (e.g. payment systems, matching services). Instead, it is a deliberately chosen business model. Spotify, for instance, runs a platform model (the advertising-financed basic version) next to a classical retail model (the subscription and user-payment-financed premium version). Thus, platform economics do not explain all elements in media markets in general and in VoD streaming markets in particular. While a video-sharing platform resembles a platform in the economic sense, an advertising-free, subscription-based on-demand audiovisual media service embraces a more traditional retail model (buying broadcasting rights from upstream suppliers and selling streaming services to one customer group – viewers – that directly pays by means of a monthly flat-rate price). Notable implications of platform economics include, inter alia, an asymmetric pricing structure where the customer group that generates the strongest indirect network effect is priced very low (possibly with a price of zero), whereas the other customer group is priced considerably higher and generates the revenue for the platform. Furthermore, indirect network effects represent demand-side economies of size, so that – in combination with other factors like direct network effects<sup>328</sup> – platform markets may tend towards a narrow oligopolistic market structure, sometimes with one company dominating the market (like in the above examples of Google Search or the Facebook Group). Thus, platforms may favour the emergence of gatekeepers through the rise of horizontal market power.

- Data economics:<sup>329</sup> One of the more marked differences between offline and online media markets is the availability and commercial employment of personalized user

---

“Competition and Antitrust in Internet Markets”, in: J.M. Bauer and M. Latzer (eds.), *Handbook on the Economics of the Internet*, Cheltenham: Edward Elgar 2016, 183-210; Rochet, J.-C. and J. Tirole, “Platform Competition in Two-sided Markets”, *Journal of the European Economic Association* 1(4), 2003, 990-1029.

<sup>326</sup> See Anderson, S.P. and J.J. Gabszewicz, “The Media and Advertising: A Tale of Two-sided Markets”, *Handbook of the Economics of Art and Culture* 1, 2006, 567-614.

<sup>327</sup> Note that the effect is not so clear in the other direction: Do viewers value more advertising?

<sup>328</sup> See Katz, M.L. and Shapiro, C., “Network Externalities, Competition, and Compatibility”, *The American Economic Review* 75(3), 1985, 424-440; Katz, M.L. and Shapiro, C., “Systems Competition and Network Effects”, *Journal of Economic Perspectives* 8(2), 1994, 93-115.

<sup>329</sup> See, inter alia, Acquisti, A., C.R. Taylor and L. Wagman, “The Economics of Privacy”, *Journal of Economic Literature* 54(2), 2016, 442-492, <http://dx.doi.org/10.1257/jel.54.2.442>; Budzinski, O. and Kuchinke, B.A., “Industrial Organization of Media Markets and Competition Policy”, in: M.B. von Rimscha (ed.), *Management and Economics of Communication*, Berlin: DeGruyter 2020, 21-45; Hirshleifer, J., “Privacy: Its Origin, Function, and Future”, *The Journal of Legal Studies* 9(4), 1980, 649-664; Kerber, W., “Digital Markets, Data, and Privacy:



data. This data includes (i) simple registration data (like email addresses, names, sex, age, residence information, account/payment information, etc.), (ii) advanced behavioral data (like individual browsing, searching, and buying histories, posts, comments, ratings/“likes”, etc.), and (iii) derived data through pooling the simple and advanced personalized data with other information including comparisons to similar individuals. The analysis of the latter yields more or less accurate individual consumption patterns from which reasonable hypotheses about individual consumer preferences may be derived. These derived hypothetical consumption patterns and preference conjectures play an important role in commercial data-based business models. They can be profitably used to, first, personalize commodities and services according to the conjectured user preference. Streaming services in particular personalize search and recommendation services (usually algorithm-based), so that users easily find content that they probably like (individually ranked search lists as a response of the system to a search enquiry) and receive recommendations about other content they are likely to enjoy (proactive individual recommendation lists).<sup>330</sup> This enhances both consumer satisfaction and the time that users spend on streaming content – increasing consumer loyalty, willingness-to-pay, personalized data supply, etc. Second, the results of the complex data analyses may be sold to interested third parties. Streaming services sell data analysis results, for instance, to companies wanting to have their advertising directed towards the attention of specific target groups (targeted advertising)<sup>331</sup> or to upstream firms like content producers (wanting to know more about what streaming consumers like and how they behave). Third, personalized data may be used for data-based price discrimination on an individual level. However, as far as I know, streaming services do not currently employ data-based price discrimination in any prominent way. Notable implications of data economics include, inter alia, the relevance of the vertical flow of information through the supply chain and the incentives to bias it. In this framework, gatekeeping emerges as the ability to control (vertical) information flows and incentives to profitably bias them – and not necessarily through traditional horizontal market power or through tendencies towards horizontal market dominance alone. Gatekeeping effects arise much earlier through vertical integration but, of course, are further aggravated by market concentration.

---

Competition Law, Consumer Law and Data Protection”, *Journal of Intellectual Property Law & Practice* 11(11), 2016, 856-866; Posner, R.A., “The Economics of Privacy”, *American Economic Review* 71(2), 1981, 405-409; Taylor, C.R., “Consumer Privacy and the Market for Customer Information”, *The RAND Journal of Economics* 35(4), 2004, 631-650; Hermalin, B.E. and Katz, M.L., “Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy”, *Quantitative Marketing and Economics* 4(3), 2006, 209-239.

<sup>330</sup> An in-depth analysis of the good “search and recommendation service” is provided by Budzinski, O., Gaenssle, S. and Lindstädt-Dreusicke, N., “Data (R)Evolution – The Economics of Algorithmic Search & Recommender Services”, forthcoming in: S. Baumann (ed.), *Handbook of Digital Business Ecosystems*, Cheltenham: Elgar 2021.

<sup>331</sup> In this case, platform economics and data economics meet. While platform economics focuses on the indirect network effect from attracting audiences to the willingness-to-pay model of advertisers, data economics frames the same phenomenon as selling information (i.e. where and how to find the targeted consumers) to a third party (indirectly, if the streaming service also provides the service of placing the ads accordingly).



- Attention economics:<sup>332</sup> At the end of the day, the audiovisual sector competes for the attention of the viewers – like many other offline and online services. While attention is scarce, the information supply within the Internet alone implies a fundamental situation of information overload. Therefore, the economics of attention imply that while bringing content to the market often doesn't face relevant (technological) barriers, attracting and maintaining attention (audience building) represents the more relevant entry barrier.<sup>333</sup> Only a fraction of audiovisual content receives so much of the consumers' attention that it actually makes it into the options for consumption decisions – and even less content is truly successful. This is further fueled by self-reinforcing effects of successful content: various network effects propel few content items into superstardom-like consumption.<sup>334</sup> Thus, consumers have an overview of only a small portion of the actual content portfolio and, consequently, de facto market transparency is low. Consumers need pre-structuring assistance in order to cope with information overload – but can only imperfectly assess the quality of such services. In particular with their algorithm-based search and recommendation systems, streaming services pre-select what is brought to the attention of the user – in a modern version of what editorial offices used to do in the traditional media world but based on markedly different selection criteria.<sup>335</sup> Notable implications of attention economics include, inter alia, that pre-structuring of information flows and pre-selecting of content is a necessary ingredient of an information-rich society. However, this requires some control over information flows and, in combination with imperfect quality-assessment competencies of consumers, generates inevitably some gatekeeping power (i.e., limited scope to bias the information flow according to profitable self-interest

---

<sup>332</sup> See, inter alia, Falkinger, J., "Limited Attention as a Scarce Resource in Information-Rich Economies", *The Economic Journal* 118(532), 2008, 1596-1620; Anderson, S.P. and A. de Palma, "Competition for Attention in the Information (Overload) Age", *The RAND Journal of Economics* 43(1), 2012, 1-25; Taylor, G., "Scarcity of Attention for a Medium of Abundance", in: M. Graham & W.H. Dutton (Eds.), *Society and the Internet: How Networks of Information and Communication are Changing Our Lives*, Oxford University Press 2014, 257-271; Che, Y.-K. and Mierendorff, K., "Optimal Dynamic Allocation of Attention", *American Economic Review* 109(8), 2019, 2993-3029, <http://dx.doi.org/10.1257/aer.20171000>; Boik, A., Greenstein, S.M. and Prince, J., "The Empirical Economics of Online Attention", Kelley School of Business Research Paper No. 22427, 2017, <http://www.nber.org/papers/w22427.pdf>; Gaenssle, S., "Attention Economics of Instagram Stars: #Instafame and Sex Sells?", *Ilmenau Discussion Papers* 27(150), 2021, <http://dx.doi.org/10.2139/ssrn.3861486>.

<sup>333</sup> See Budzinski, O. and Gaenssle, S., "The Economics of Social Media (Super-)Stars: An Empirical Investigation of Stardom and Success on YouTube", *Journal of Media Economics* 31(3-4), 2020, 75-95, <https://doi.org/10.1080/08997764.2020.1849228>; Gaenssle, S., "Attention Economics of Instagram Stars: #Instafame and Sex Sells?", *Ilmenau Discussion Papers* 27(150), 2021, <http://dx.doi.org/10.2139/ssrn.3861486>.

<sup>334</sup> See with respect to online content Budzinski, O. and Gaenssle, S., "The Economics of Social Media (Super-) Stars: An Empirical Investigation of Stardom and Success on YouTube", *Journal of Media Economics* 31(3-4), 2020, 75-95, <https://doi.org/10.1080/08997764.2020.1849228>; Gaenssle, S. and Budzinski, O., "Stars in Social Media: New Light Through Old Windows?", *Journal of Media Business Studies* 18(2), 2021, 79-105, <https://doi.org/10.1080/16522354.2020.1738694>.

<sup>335</sup> See Budzinski, O., Gaenssle, S. and Lindstädt-Dreusicke, N., "Data (R)Evolution – The Economics of Algorithmic Search & Recommender Services", forthcoming in: S. Baumann (ed.), *Handbook of Digital Business Ecosystems*, Cheltenham: Elgar 2021; Belleflamme, P. and Peitz, M., "Ratings, Reviews, Recommendations and the Consumption of Cultural Goods", in: R. Towse and T. Navarrete Hernández (eds.), *Handbook of Cultural Economics*, 3<sup>rd</sup> Edition, Cheltenham: Elgar 2020, 466-473.



without the consumer noticing<sup>336</sup>) – irrespective of market power. The concentration of content that is brought to the attention of the consumers is, on the one hand, limited by the personalisation and individualisation of search and recommendation services (enhancing the range of top-listed content across users) but, on the other hand, promoted by content-related superstar effects and the desire of consumers for one-stop shopping and single-homing, i.e. avoiding the burdensome handling of multiple subscriptions to various streaming services.

The following discussion of gatekeeping effects in VoD markets draws on these theory elements.

### 7.3. Competition and gatekeeping in streaming markets

Currently, VoD markets are characterised by intensive competition and frequent newcomers to the market.<sup>337</sup> As such, the more sclerotic market structures of traditional television have been upset by a wave of new competition from the various types of online streaming services. This increase of competitive pressure and re-vitalization of competition in the audiovisual sector is welcome from a social welfare perspective. However, does the absence of a single market dominator like in the markets for search engines or social network services automatically imply that no gatekeeper power exists in VoD/streaming markets? If the underlying economic thinking is restricted to platform economics, horizontal market power indeed becomes paramount for gatekeeping power that can be anticompetitively abused. Only if the competition among platforms is not sustainable, is one platform likely to dominate at the end of the day. In other words, only if the characteristics of streaming markets sufficiently favor platform size, is gatekeeping through horizontal market power likely to emerge in the future. On the one hand, it is unclear and probably doubtful whether direct and indirect network effects are strong enough to fuel a dynamic towards an inevitable dominant streaming platform in the long run. On the other hand, potentially strong preferences for single-homing and one-stop shopping as well as strategic elements like artificial incompatibilities between platforms and deliberately increased switching costs may favor a concentration process towards a single dominant streaming platform (in the long run, as it is clearly not on the horizon in the short run). Moreover, when it comes

---

<sup>336</sup> If the deviation from optimal search results and recommendations is sufficiently small, consumers will not notice a loss in quality and not leave the service. Furthermore, the sensitivity of consumers (recommendation elasticity of demand) will differ interpersonally. See Budzinski, O., Gaenssle, S. and Lindstädt-Dreusicke, N., “Data (R)Evolution – The Economics of Algorithmic Search & Recommender Services”, forthcoming in: S. Baumann (ed.), *Handbook of Digital Business Ecosystems*, Cheltenham: Elgar 2021.

<sup>337</sup> See Aguiar, L. and Waldfogel, J., “Netflix: Global Hegemon or Facilitator of Frictionless Digital Trade?”, *Journal of Cultural Economics* 42(3), 2018, 419-445, <https://doi.org/10.1007/s10824-017-9315-z>; Lindstädt-Dreusicke, N. and Budzinski, O., “The Video-on-demand Market in Germany – Dynamics, Market Structure and the (Special) Role of YouTube”, *Journal of Media Management and Entrepreneurship* 2(1), 2020, 108-123, <http://dx.doi.org/10.4018/JMME.2020010107>; Budzinski, O. and Lindstädt-Dreusicke, N., “Antitrust Policy in Video-on-Demand Markets: The Case of Germany”, *Journal of Antitrust Enforcement* 8(3), 2020, 606-626, <https://doi.org/10.1093/jaenfo/jnaa001>; Budzinski, O., Gaenssle, S. and Lindstädt-Dreusicke, N., “The Battle of YouTube, TV and Netflix – An Empirical Analysis of Competition in Audio-visual Media Markets”, *Ilmenau Economics Discussion Papers* 26(137), 2020, <http://dx.doi.org/10.2139/ssrn.3569553>.



to digital goods, distances and geography do not cause relevant costs anymore, so that the scope for separated regional markets is eroded –with the exception of remaining language and cultural barriers.<sup>338</sup> Therefore, it is understandable that a platform-centric view denies relevant or urgent gatekeeper concerns in streaming markets.

However, modern insights from data economics and attention economics change the perspective. Horizontal market power, in this view, certainly aggravates the gatekeeper concerns, yet gatekeepers are likely to emerge in relevant ways already way below any common market dominance threshold. Data economics points to the relevance of vertical integration as a sufficient condition for welfare-decreasing gatekeeping concerns.<sup>339</sup> As soon as streaming services are united with upstream content producers, they experience incentives to abuse their gatekeeper position. Such abuses may consist of foreclosure strategies like denying competing upstream contents access to the streaming service (blackout of upstream competitors or delisting of their content), a strategy that is especially viable against fringe and maverick competitors in the upstream content markets. A similar effect may be achieved through discriminatory access conditions, including data-based variants like blocking the transmission of sales data or customer information to competitors of own-content producers on the upstream level.<sup>340</sup>

Slightly more elegant is self-preferencing, or using search and recommendation systems to steer the audience towards own/related content and away from the content of the closest competitors. Competition by other streaming services limits the scope for gatekeeper behavior like this but only to a limited extent. For consumers to actually react to search and recommendation bias, they would need to become aware of the marginally reduced search and recommendation quality (i.e. the marginally lower fit to their preferences) if these services become biased for self-preferencing reasons. However, attention economics tell us that consumers are unlikely to have the necessary clear view in situations of information overflow. In the context of VoD, consumers will realize that performance is bad when they do not like the results of their search enquiries (i.e. if they do not find what they are searching for) and/or the recommended content. However, they will often not know whether something even better is hidden in the hundreds or millions

---

<sup>338</sup> See Gaenssle, S. et al., “Conquering the Box Office: Factors Influencing Success of International Movies in Russia”, *Review of Network Economics* 17(4), 2019, 245-266, <https://doi.org/10.1515/rne-2019-0017>.

<sup>339</sup> See also the recent economic theory literature on when incentives for foreclosure and/or self-preferencing occur: Bourreau, M. and Gaudin, G., “Streaming Platform and Strategic Recommendation Bias”, 2018, <https://ssrn.com/abstract=3290617>; Crawford, G.S., Lee, R.S., Whinston, M.D. and Yurukoglu, A., “The Welfare Effects of Vertical Integration in Multichannel Television Markets”, *Econometrica* 86(3), 2018, 891-954, <https://doi.org/10.3982/ECTA14031>; De Cornière, A. and Taylor, G., “A Model of Biased Intermediation”, *The Rand Journal of Economics* 50(4), 2019, 854-882, <https://doi.org/10.1111/1756-2171.12298>; Hagiu, A., Teh, T.-H. and Wright, J., “Should Platforms be Allowed to Sell on their Own Marketplaces?”, Working Paper, 2020, [http://andreihagiu.com/wp-content/uploads/2020/08/DualModePlatform\\_20200818.pdf](http://andreihagiu.com/wp-content/uploads/2020/08/DualModePlatform_20200818.pdf); Padilla, J., Perkins, J. and Piccolo, S., “Self-Preferencing in Markets with Vertically-Integrated Gatekeeper Platforms”, *CSEF Working Paper* 582, 2020, <http://dx.doi.org/10.2139/ssrn.3701250>; Marty, F., “Competition and Regulatory Challenges in Digital Markets: How to Tackle the Issue of Self-Preferencing”, GREDEG Working Paper, 2021, <http://www.gredeg.cnrs.fr/working-papers/GREDEG-WP-2021-20.pdf>.

<sup>340</sup> See Salop, S.C., “Invigorating Vertical Merger Enforcement”, *The Yale Law Journal* 127(7), 2018, 1962-1994; Bougette, P., Budzinski, O. and Marty, F., “Exploitative Abuse and Abuse of Economic Dependence: What Can We Learn from an Industrial Organization Approach?”, *Revue d'Economie Politique* 129(2), 2019, 261-286, [https://www.cairn-int.info/article.php?ID\\_ARTICLE=E\\_RED\\_P\\_292\\_0261](https://www.cairn-int.info/article.php?ID_ARTICLE=E_RED_P_292_0261); Stöhr, A. et al., “Happily Ever After? Vertical and Horizontal Mergers in the US Media Industry”, *World Competition* 43(1), 2020, 135-162.



of down-ranked items if the recommended content is sufficiently to their liking. Thus, some biasing is likely to be always possible – and its scope grows with the depth of vertical integration and the weakening of competition forces. Nonetheless, it requires some vertical integration (or vertical contracts prioritizing specific content suppliers) to create the incentives to profitably engage in anticompetitive gatekeeping. As a consequence, departing from a purely platform-centric view and embracing a more comprehensive modern economics perspective draws a less optimistic picture about the absence and probability of gatekeeping power in the audiovisual sector.

As already mentioned in the beginning of this section, competition is dynamic and intense in VoD markets at the time of writing. However, some recent merger and acquisition developments are relevant for the prospects of gatekeeping power in streaming markets and in the audiovisual sector as a whole:

- Horizontal megamergers like Disney/Fox (cleared in 2018) have ignited an ongoing concentration process at the upstream market stages of the audiovisual sector.<sup>341</sup> The media conglomerate is also active at the streaming/VoD stage of the supply chain (Disney+, Hulu).
- Following the merger of Comcast and NBCU already in the early 2010s, the vertical merger of telecommunications company AT&T and content giant Time Warner (cleared in 2018) created another vertically integrated company that covers the whole supply chain from content production (WarnerMedia) through streaming/television distribution (HBO Max, Turner Networks) to Internet/cable access providers (AT&T).<sup>342</sup> In the US television market, the employment of blackout strategies, as a consequence, was already observable.<sup>343</sup>
- Additionally, the leading streaming services are also striving for vertical integration. Next to the upstream endeavors of streaming services (investment in own productions), Amazon appears close to acquiring MGM studios in 2021.<sup>344</sup>
- Also in 2021, the two biggest private French broadcasters, TF1 and M6, have announced a merger in order to respond to the concentration race in the audiovisual sector and the rise of streaming services by forming a “national champion”. This goes hand-in-hand with calls for European-wide alliances of commercial broadcasters.<sup>345</sup>

---

<sup>341</sup> See Stöhr, A. et al., “Happily Ever After? Vertical and Horizontal Mergers in the US Media Industry”, *World Competition* 43(1), 2020, 135-162.

<sup>342</sup> See Salop, S.C., “Invigorating Vertical Merger Enforcement”, *The Yale Law Journal* 127(7), 2018, 1962-1994; Salop, S.C., “The AT&T/Time Warner Merger: Judge Leon Garbled Professor Nash”, *Journal of Antitrust Enforcement* 6, 2018, 459-469, <https://doi.org/10.1093/jaenfo/jny016>; Stöhr, A. et al., “Happily Ever After? Vertical and Horizontal Mergers in the US Media Industry”, *World Competition* 43(1), 2020, 135-162.

<sup>343</sup> See Stöhr, A. et al., “Happily Ever After? Vertical and Horizontal Mergers in the US Media Industry”, *World Competition* 43(1), 2020, 135-162, pages 145, 154, 160.

<sup>344</sup> See CPI, “Amazon Nears Deal to Buy MGM Studios For \$9B”, <https://www.competitionpolicyinternational.com/amazon-deal-to-buy-mgm-studios-for-9b-nearly-done/>.

<sup>345</sup> See CPI, “French Broadcasters Merge to Compete with US Netflix”, <https://www.competitionpolicyinternational.com/french-broadcasters-merge-to-compete-with-us-netflix/>.



- Again in 2021, AT&T-Time Warner plans to further expand with the acquisition of Discovery (content, television channels, and streaming services).<sup>346</sup>

This dynamic horizontal and vertical integration process is very likely to significantly increase the possibility, scope, and incentives to use gatekeeping power in anticompetitive ways.

In summary, the twin occurrence of vertical integration and control over audience building (i.e. access to attention) promotes gatekeeping power in the audiovisual sector. The latter is unavoidable to some degree as pre-structuring assistance for video consumers is necessary in an information overload world where attention is a scarce good. Since some gatekeeping power is inherent to digital streaming services, the incentives to employ it for self-preferencing and biasing the steering of consumers' attention becomes crucial. Vertical integration automatically generates such biasing incentives as soon as it includes the market stage of streaming services (and is further increased if, additionally, the market stage of Internet access providers is part of it as well). Then, the scope and incentives for anticompetitive gatekeeping are present. Market concentration at any stage of the supply chain further increases the problem.

## 7.4. Regulatory implications for audiovisual streaming markets from an economic perspective

On-demand audiovisual media services are outside the scope of the DSA package<sup>347</sup>, even though from an economic perspective, as argued in the preceding sections, gatekeeping power is likely to exist in digital audiovisual markets and to generate relevant economic effects. But what if the package did apply to such services? In this section, I pick up selected regulatory ideas from the DSA package and analyze in a “what if-scenario” whether they could serve as paragons for alleviating gatekeeping concerns in video-streaming markets. Looking into the economics of gatekeeping in the audiovisual sector reveals two major concerns: first, self-preferencing, and second, vertical integration (in particular if it includes either the market stage of streaming services or the market stage of Internet access providers). Both concerns do not depend on the company enjoying a dominant position in a relevant market.

### 7.4.1. Self-Preferencing

The DSA package addresses the issue of self-preferencing. A core platform service provider (defined in Art. 2 and 3 DMA) is obliged to refrain from self-preferencing (Art. 6(1)(d) DMA) and “very large” online services are required to provide some transparency regarding the

---

<sup>346</sup> See CPI, “AT&T, Discovery Agree to Merger of CNN”, <https://www.competitionpolicyinternational.com/att-discovery-agree-to-merger-of-cnn/>.

<sup>347</sup> See Article 2(2) DMA.



main parameters employed in their recommender systems (Art. 29 DSA).<sup>348</sup> Furthermore, the DSA package is designed to ‘only’ capture the largest online services, essentially the so-called GAFAM companies (Google, Apple, Facebook, Amazon, Microsoft), by setting absolute-size thresholds in particular with respect to proxy size.<sup>349</sup>

Interestingly, in doing so, the DSA package moves away from concepts like the dominance of an exactly delineated relevant market.<sup>350</sup> Given the analysis in this paper, looking beyond traditional dominance concepts is also relevant when it comes to gatekeeping in the audiovisual sector (see §7.3). However, generally, the DSA package adopts a gatekeeper notion that is predominantly driven by platform economics and, thus, deviates from the concept of gatekeeping prominently used in media (see §7.2). Therefore, even if the DSA package were to apply to on-demand audiovisual media services, at least some of the relevant players with gatekeeping power in the audiovisual sector would still escape the new regulation. From an economic point of view, it is somehow puzzling that Art. 2(2) DMA lists “video-sharing platform services” but not video-streaming services in general. Given the close competitive interrelation between these different types of services (see §7.1), referring to some players within a market but not the others (at the end of the day differentiated by a choice of business model more than anything else) appears to be doubtful from an economic perspective and seems to be driven by the platform economics-focused perspective (potentially neglecting the insights from data and attention economics). In line with other economics assessments, an unambiguous black-listing of self-preferencing behaviour by gatekeepers (irrespective of how they organize their business and independent from traditional market dominance concepts) could be justified from an economic perspective.<sup>351</sup>

Another interesting approach is constituted by rules against the discrimination of business users of platforms in the DSA package (Art. 5 and 6 DMA). Due to the complexity of algorithm-based search recommendation rankings, however, a non-discrimination rule in this general sense may be difficult to apply *ex ante* (in a sector regulation style) and

---

<sup>348</sup> Writing from an economic perspective, I refrain from legal interpretations in relation to the audiovisual sector and specific VoD services. See, for instance, Chapter 6 of this publication for such an exercise. See also Podszun, R., Bongartz, P. and Langenstein, S., “Proposals on how to Improve the Digital Markets Act”, Policy paper in preparation for the information session on the Digital Markets Act in the European Parliament’s Committee on Internal Market and Consumer Protection (IMCO) on 19 February 2021, <https://ssrn.com/abstract=3788571>; Vezzoso, S., “The Dawn of Pro-Competition Data Regulation for Gatekeepers in the EU”, 2021, <https://ssrn.com/abstract=3772724>; Geradin, D., “What Is a Digital Gatekeeper? Which Platforms Should Be Captured by the EC Proposal for a Digital Markets Act?” 2021, <https://ssrn.com/abstract=3788152>; Leistner, M., “The Commission’s Vision for Europe’s Digital Future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act – A Critical Primer” 2021, <https://ssrn.com/abstract=3789041>.

<sup>349</sup> See, inter alia, Cabral, L. et al., “The Digital Markets Act: A Report from a Panel of Economic Experts”, Luxembourg: European Union 2021, page 9, <http://dx.doi.org/10.2760/139337>.

<sup>350</sup> See on the critical economic view of over-reliance on market delineation, inter alia, Farrell, J. and Shapiro, C., “Antitrust Evaluation of Horizontal Mergers: An Economic Alternative to Market Definition”, *The B.E. Journal of Theoretical Economics* 10(1), 2010, 1-40, <https://faculty.haas.berkeley.edu/shapiro/alternative.pdf>; Kaplow, L., “Market Definition and the Merger Guidelines”, *Review of Industrial Organization* 39(1-2), 2011, 107-125, <https://link.springer.com/article/10.1007/s11151-011-9305-9>; Kaplow, L., “Market Definition, Market Power”, *International Journal of Industrial Organization* 43(C), 2015, 148-161, <https://doi.org/10.1016/j.ijindorg.2015.05.001>.

<sup>351</sup> See, inter alia, Cabral, L. et al., “The Digital Markets Act: A Report from a Panel of Economic Experts”, Luxembourg: European Union 2021, <http://dx.doi.org/10.2760/139337>.



enforcement may need to rely more on *ex post* intervention (in a competition policy style).<sup>352</sup> It is important that the notion of non-discrimination does not extend beyond preventing self-preferencing since every preference-oriented (and actually every non-random) ranking and recommendation system is to some extent discriminatory – for instance, in the ideal and mostly beneficial<sup>353</sup> case, discriminating against content that the algorithmic estimation of what the consumer wants deems to be less fitting.

Similarly, transparency requirements for streaming services regarding the parameters determining algorithmic search and recommendation rankings – as exemplarily laid out in the DSA – would be ambivalent from an economic perspective if they applied to on-demand audiovisual media services. While they may help consumers to understand what they are facing, they also constitute parameters of socially beneficial competition between VoD services. The incentives to improve individualised search and recommendation services – innovation dynamics that may especially benefit non-mainstream consumers in the future as this is where remaining room for improvement may be particularly located – should not be eroded by (too-) far-reaching transparency requirements. In particular, a scenario where the value of quick search and comfortable consumption decisions is eroded by lengthy educational interfaces that first have to be “clicked away” would be unwelcome from an attention economics perspective. The helping hand for consumers facing information overload would then be weakened. On the other hand, more voluntary options to influence the weights of different parameters for one’s own personalised search and recommendation rankings (without consumers being forced to self-adapt them) could possibly increase consumer welfare.

## 7.4.2. Vertical Integration

While some of the markets addressed by the DSA package are already characterised by dominant gatekeepers, the audiovisual sector is still in a state of dynamic competition. Thus, it is important to actively protect the competitive process here, instead of waiting until a dominant gatekeeper has established itself and then throw the regulatory package at it. Preventing the incentives for an anticompetitive use of gatekeeping power, which surface through vertical integration (covering streaming services and/or Internet access), is more effective than regulating dominant gatekeepers given the ubiquitous enforcement difficulties (but not impossibilities!) accompanying a (recommendable) ban on self-preferencing (and further regulation). This would require including merger control as an *ex ante* instrument to prevent potentially anticompetitive market structures from obstructing the regulatory framework’s ability to address gatekeeping power. The DSA package remains

---

<sup>352</sup> See Cabral, L. et al., “The Digital Markets Act: A Report from a Panel of Economic Experts”, Luxembourg: European Union 2021, <http://dx.doi.org/10.2760/139337> as well as Budzinski, O., Gaenssle, S. and Lindstädt-Dreusicke, N., “Data (R)Evolution – The Economics of Algorithmic Search & Recommender Services”, forthcoming in: S. Baumann (ed.), *Handbook of Digital Business Ecosystems*, Cheltenham: Elgar 2021.

<sup>353</sup> Even then, concerns about cultural consumption bubbles may be considered. See Budzinski, O., Gaenssle, S. and Lindstädt-Dreusicke, N., “Data (R)Evolution – The Economics of Algorithmic Search & Recommender Services”, forthcoming in: S. Baumann (ed.), *Handbook of Digital Business Ecosystems*, Cheltenham: Elgar 2021.



largely silent on merger control, especially with respect to preventing and limiting gatekeeper power.<sup>354</sup> Thus, this area lies clearly outside the scope of the DSA package.

Addressing the ongoing wave of vertical integration in the audiovisual sector (see §7.3) that is generating worrying gatekeeping power, requires reinvigorating the control of vertical and conglomerate mergers, particularly in the audiovisual sector (but also generally in the digital economy).<sup>355</sup> The focus on horizontal mergers and the accompanying leniency with regard to non-horizontal company combinations may have been justified by efficiency considerations in traditional brick-and-mortar markets. In the digital online world, however, the anticompetitive impact of vertical integration can be much more severe, and it matters which market stages a vertical integration covers. Market stages where the attention of the audience is channeled and directed – often in data-based ways – are particularly sensitive when it comes to the generation of anticompetitive incentives through vertical integration. A more restrictive merger control, focusing on incentives for anticompetitive gatekeeping rather than on theoretical marginal efficiency gains, would be beneficial from an economic perspective.

Notwithstanding the crucial relevance of vertical integration, active merger control preventing horizontal power is also relevant, as market concentration aggravates gatekeeping power. The current wave of mega-mergers in the audiovisual sector is already changing market structure in a way that generates incentives for increasing gatekeeping behavior.

### 7.4.3. Summary

In summary, competition dynamics in the audiovisual sector are sensitive and require protection. Gatekeeping power is inherent to streaming markets and inevitably accompanies the beneficial pre-structuring assistance necessary in an information overload world. Therefore, it would be welfare-decreasing to wait for a dominant company to “tip” the market and then place it under specific gatekeeper regulation. Instead, addressing gatekeeper issues in video-streaming markets, for instance with a combination of (i) competition policy instruments (merger control) preventing problematic horizontal and especially vertical structures and (ii) behavioral regulation of gatekeeping power banning self-preferencing and discriminatory access to sales and customer information, would offer the best chance of protecting socially beneficial competition in the audiovisual sector – including its diversity and smaller market participants at different market stages. This would also best approximate a fair level-playing field. From an economic perspective, some ideas and concepts from the DSA package could serve as paragons here. However, beyond

---

<sup>354</sup> See also Cabral, L. et al., “The Digital Markets Act: A Report from a Panel of Economic Experts”, Luxembourg: European Union 2021, <http://dx.doi.org/10.2760/139337> as well as more generally on the important role of merger control in combating the power of online gatekeepers Budzinski, O., Gaenssle, S. and Stöhr, A., “Outstanding Relevance across Markets: A New Concept of Market Power?”, *Concurrences* 17(3), 2020, 38-43.

<sup>355</sup> See Salop, S.C., “Invigorating Vertical Merger Enforcement”, *The Yale Law Journal* 127(7), 2018, 1962-1994; Stöhr, A. et al., “Happily Ever After? Vertical and Horizontal Mergers in the US Media Industry”, *World Competition* 43(1), 2020, 135-162.



this, activation and reinvigoration of merger control would be beneficial from an economic perspective.

## 8. Summaries of the series of EAO events on the DSA Package<sup>356</sup>

This section briefly summarises the discussions from the series of events organised and moderated by the European Audiovisual Observatory from February to July 2021 on the DSA Package.<sup>357</sup>

- “The new Digital Services Act Package: A paradigm shift?”, 11 February 2021;
- “Transparency of content moderation on social media”, 18 March 2021;
- “Gatekeepers in the DSA Package: What about VoD?”, 22 April 2021;
- “Copyright and the DSA”, 27 May 2021;
- “The DSA and the fight against disinformation”, 1 July 2021.

The summaries reflect only the main points of the discussions, so any statement of intervening participants should be checked against delivery as per the recordings made available for each event on the website of the Observatory.

The experts invited to introduce the topics of the events have authored the chapters of this publication.

### 8.1. A first look at the new EU rules on online services and their possible impact on the audiovisual industry<sup>358</sup>

#### 8.1.1. Setting the scene: Overview of the new Digital Services Act Package

Francisco Cabrera, Senior Legal Analyst at the Department for Legal Information (EAO), introduced the conference by describing the evolution of the European legal framework regulating online platforms, starting with the e-Commerce Directive 2000/31/EC. This Directive introduced a limited liability regime for Internet service providers, while

---

<sup>356</sup> The summaries have been drafted by Léa Chochon, Junior Analyst at the European Audiovisual Observatory.

<sup>357</sup> The kick-off conference <https://www.obs.coe.int/en/web/observatoire/-/the-new-digital-services-package-a-paradigm-shift-> and the four webinars <https://www.obs.coe.int/en/web/observatoire/-/series-of-webinars-from-march-to-july> were all conceived by the team of analysts of the Department for Legal Information of the European Audiovisual Observatory (Francisco Cabrera, Julio Talavera and Sophie Valais) and moderated by Maja Cappello, Head of the Department for Legal Information at the Observatory.

<sup>358</sup> This section briefly summarises the discussions from the introductory conference “The new Digital Services Act Package: A paradigm shift?”, 11 February 2021, <https://www.obs.coe.int/en/web/observatoire/-/the-new-digital-services-package-a-paradigm-shift->. The summary reflects only the main points of the discussions, so please check upon delivery: the recording of the conference is available at: <https://www.youtube.com/watch?v=eqFLGiTsnFO>.



remaining unchanged for over 20 years. Hence, for obvious reasons, it has been unable to keep up with the new types of services that have emerged since its adoption. This EU legislation was then supplemented by other legal tools, such as the EU's Audiovisual Media Services (AVMS) Directive 2018/1808 and the Copyright in the Digital Single Market (DSM) Directive (EU) 2019/790, but neither of them have a similar scope. In 2019 the European Commission launched the process of adopting a broader legal framework, leading to the Digital Services Act (DSA) Package. The new legislative proposal was presented in December 2020 and consists of two regulations: the Digital Services Act, which provides basic rules for intermediary services offering network infrastructure, and further and specific rules for identified sub-categories such as hosting providers, online platforms and very large platforms; and the Digital Markets Act (DMA), which focuses on "gatekeepers", through the prohibition of a number of unfair practices, the obligation to proactively put in place certain measures, the imposition of sanctions in case of non-compliance, etc.

### 8.1.2. The experts' corner: Competition, liability and interaction between the DSA Package, the AVMS Directive and the DSM Directive

The first intervention saw Mark Cole, Professor for Professor for Media and Telecommunication Law at the University of Luxemburg and Director for Academic Affairs at the Institute of European Media Law (EMR), look at the notion of gatekeepers and competition within the DMA. Articles 2 and 3 of the DMA define a gatekeeper as a provider of core platform services, meaning it has a significant impact on the internal market, serves as an important gateway for businesses in their interaction with consumers, and enjoys or is likely to enjoy an entrenched and durable position. Numerical criteria such as turnover or customer reach complete this definition. Furthermore, although the objective of the DMA was thought to be closely related to competition, its legal basis is anchored to the internal market and to Article 114 TFEU. It thus aims at creating a contestable and fair market in the digital sector, by setting up measures to make it more transparent and open to all. Such measures include more transparency on data related to online platforms (e.g. on advertising schemes or profiling techniques) and more access to performance-measuring tools. The DMA also provides for a significant increase in the Commission's enforcement powers including sanctioning powers.

The second presentation, provided by Joan Barata, Intermediary Liability Fellow at Stanford Law School, focused on the evolution of the exemption liability regime, starting with the e-Commerce Directive regime which incentivised platforms to take a passive approach to moderation of online content in order to retain liability exemption, differently from the Good Samaritan clause of US tradition. The DSA partly replicated this regime but introduced other obligations such as the obligation for platforms to assess the systematic risks they create and to adopt certain measures accordingly, applicable to both illegal and harmful content. The DSA also provides that adopting a proactive attitude does not automatically result in the loss of immunity, which suggests a form of Good Samaritan approach.



In the third intervention, Martin Senftleben, Professor of Intellectual Property Law and Director of the Institute for Information Law (IViR) at the Amsterdam Law School, presented in more detail the interaction between the DSA, the AVMS Directive and the DSM Directive. In principle, Article 1(5) of the DSA provides that the rules of the DSA are without prejudice to several specific legislations. This can translate as a *lex specialis* approach but in a complementary way, meaning that specific interfaces can exist between the different instruments, and clarifications and additional measures can be introduced by the DSA to areas of regulation already dealt with by the DSM or the AVMS Directive. This is, for instance, the case in the area of tackling harmful content, where the DSA introduces measures such as trusted flaggers or risk assessment and mitigation obligations for very large online platforms.

### 8.1.3. The stakeholders' panel: The DSA, a much-needed update of an outdated legal framework

To launch the discussion, representatives of the European Commission presented the principles of the regulatory approach behind the DSA. Firstly, the regulation of online content must be designed to respect fundamental rights, in particular freedom of expression. Secondly, a balance must be struck between private and public enforcement, ensuring a sufficient level of public enforcement in the way content moderation standards are defined and applied online. Regarding those standards, the representatives reported that the AVMS Directive should remain the main reference framework for moderating harmful content, including the protection of minors. The DSA will then provide this overall structure and fill some of the gaps. Three important issues were raised with regard to interaction of the DSA Package with other instruments such as the recently adopted action plans:<sup>359</sup> cooperation between authorities in relation to illegal content online; overall transparency on online advertising; and the promotion of European works.

In general, all stakeholder representatives acknowledged the need to update the regulatory framework for online platforms and welcomed it for various reasons. However, the complexity of the provisions of the DSA Package, its scope and its interaction with other legal instruments were pointed out several times. From the perspective of the public service broadcasters, it was suggested that this new regulatory framework allows for fairer competition in the digital space and a more accountable and transparent online environment. They also highlighted the importance of the DMA's prohibition of unfair and discriminatory practices, which aims to protect and prevent the misuse of public broadcasters' data by high-tech companies, but also pointed out the need to clearly delineate the scope of the different sectoral EU rules. In addition, they called for the DSA to protect professional edited broadcast content that is carefully regulated at the national level, as private platforms should not be able to remove such content or "re-regulate" it according to their own private business standards. On the creative side, the representatives

---

<sup>359</sup> The European Democracy Action Plan ([https://ec.europa.eu/commission/presscorner/detail/en/IP\\_20\\_2250](https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2250)) and the Action Plan to support recovery and transformation of the media and audiovisual sectors ([https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_2239](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2239)).



of authors debated the potential impact of the DSA on the issue of the balance between freedom of artistic expression and the proper valorisation of intellectual property. More specifically, they questioned the added value of the DSA with regard to the current legal framework against online piracy, and whether these new rules on gatekeepers will provide further audience data transparency between rightsholders and platforms.

Representatives of commercial broadcasters welcomed the provisions on greater transparency for online intermediaries, regulatory oversight, and potential access by researchers to the data of these large platforms. However, they identified some vulnerabilities such as the instruments for combating online piracy with the exclusion of micro-enterprises and SMEs from certain obligation, and the limited scope of the "know your business customer" (KYBC) provisions. On the regulatory side, representatives of national regulatory authorities in the media field (media NRAs) called for a clearer demarcation, in terms of supervision and regulation, between the types of services that deal with media content and those that are more market-like; they also said more information is required regarding the digital services coordinators and the scope of their remit.

Representatives of online platforms expressed their satisfaction that the liability exemption regime and the absence of a general monitoring obligation have been maintained and complemented in the DSA. This allows for some harmonisation among EU countries, and a certain level of clarity and legal certainty for businesses. They also expressed concern about the challenges of moderating online content, and the importance of transparency and user safety across the ecosystem, while raising the risk that the exclusion of small platforms from certain obligations could lead to a migration of harmful content to such platforms. Representatives of media NRAs explained that the specificities of content regulation require a tailored approach, and therefore argued for a liability regime that goes beyond the Good Samaritan principle and is more similar to a graduated system.

## **8.2. Webinar #1 - Transparency of content moderation on social media<sup>360</sup>**

### **8.2.1. Setting the scene**

Francisco Cabrera, Senior Legal Analyst of the Department for Legal Information (EAO), kicked off the webinar by giving a contrasted assessment of the state of freedom of expression and access to information in today's society. To paraphrase Charles Dickens, it is the "best of times", regarding the possibility offered by the Internet to share thoughts

---

<sup>360</sup> This section briefly summarises the discussions from the first webinar "Transparency of content moderation on social media", 18 March 2011, <https://www.obs.coe.int/en/web/observatoire/-/series-of-webinars-from-march-to-july>. The summary reflects only the main points of the discussions, so please check upon delivery: the recording of the conference is available at <https://youtu.be/c0s9nEbEdT0>.

and opinions instantly with so many people, but the “worst of times”, with respect to the increase of the level of mistrust we currently witness in public institutions and media.<sup>361</sup>

In all this, social media services play a central role as they enable billions of people to interact in an unprecedented way; at the same time they can also filter and rank information according to their own internal policies, within the limits set by the applicable legal framework. At EU level, this legal framework is based on the e-Commerce Directive and is supplemented by specific EU legislation such as the AVMS Directive and the DSM Directive. To complete this legal framework, the DSA Package sets out clear due diligence obligations for certain intermediary services and higher standards of transparency and accountability in online content moderation.

## 8.2.2. The expert’s corner: Online platforms’ moderation of illegal content online

Prof. Alexandre de Stree, University of Namur, Academic Co-director at the Centre on Regulation in Europe (CERRE), presented the main challenges of moderating online content, and how the DSA proposal attempts to address them. The first challenge lies in finding a balance between stimulating innovation and ensuring that the Internet becomes safer than it is today. The DSA allows this in a way, by maintaining the liability exemption regime, which enables innovation, and adding some new due diligence obligations, which ensure a safer Internet. The second challenge, in his view, is to have a regulation that can adapt to the different risks that online content and platforms may entail. The DSA therefore proposes a standard regime, applicable to all types of illegal content, supplemented by a set of rules differentiated according to the size of the platform, thus giving more responsibility to the largest platforms. The question of these large global platforms leads to the third challenge: the issue of enforcement. For this, the DSA proposal introduces a completely new approach in the digital sector, namely the possibility to ensure enforcement at the European level by the European Commission, rather than at the national level.

The latter challenge is also linked to the rapidly changing nature of the platforms, which requires rapid adaptation and intervention to counter illegal content, including the use of AI tools to perform part of this task. The oversight and the enforcement of content moderation rules must therefore take the form of a kind of “ecosystem”, involving not only media NRAs, but also platforms, through a number of internal compliance mechanisms, and civil society, through trusted flaggers and vetted researchers who will be able to benefit from more data transparency.

Regarding the new “Europeanised” version of the Good Samaritan clause, the expert indicated that this increases the incentive for an effective and rapid intervention by platforms, but on the condition that independent public courts (and not private platforms) have the final say on what constitutes an illegal content. One way forward, not yet included in the proposal, could be to make compliance with these due diligence obligations a

---

<sup>361</sup> See Edelman Trust Barometer 2021, <https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021%20Edelman%20Trust%20Barometer.pdf>



condition for exemption from liability. Finally, the expert stressed the need to limit the scope of the DSA to illegal content and not to include also harmful content, which would raise a number of additional fundamental rights questions and difficulties.

### 8.2.3. The stakeholders' panel: Content moderation from the perspective of platforms, consumers and media NRAs

Stakeholder representatives discussed the functioning and challenges of online moderation, including what can work, what needs to be improved, and what the DSA can bring to the table. Representatives from the field of online trust and safety shared their recommendations on the implementation and development of online moderation activities. A good common basis, regardless of the size of the platform or its location, would be to put in place from the beginning a set of company-specific values, which would then be reflected in the way the companies produce the product or service, and in the way they moderate it.

On the regulatory side, representatives from media NRAs shared how they are preparing for the new rules in the DSA Package, but also for implementation of the AVMS Directive's provisions regarding the new obligations of VSPs. They pointed out a similarity between these two instruments, which both propose a type of systemic regulation that does not focus on every single item made available on these platforms, but rather on the way platforms systematically handle content. The role of media NRAs in this regard will be to oversee the type of moderation measures adopted by platforms, how they are implemented and their effectiveness. They expressed concerns regarding the function of "digital services coordinator" introduced by the DSA Package, and whether or not it will be efficient given the extended scope of intervention.

Several representatives echoed the idea of an ecosystem of oversight mentioned by the expert and suggested that the role and tasks of the content moderators could be facilitated when complemented by trusted flaggers and the use of AI tools. Some added that the same should apply to the development of moderation standards. The representatives of civil society also pointed out that the role of civil society is essential and should be formalised in a way. However, they cautioned against the exclusive use of AI, or the use of an under-qualified human workforce, as these can lead to abuses or ethical issues in moderation. They gave the example of the results of a recent study which showed that sentences like "*As a Black woman, I agree with the previous comment*" is 10 times more likely to be removed than "*As a French man, I agree with the previous comment*".<sup>362</sup>

Other risks related to online moderation were considered, such as the risk that when a certain type of abuse or harmful content has been effectively moderated on one platform, it tends to simply move to another platform that is less moderated or defended. Other panellists touched upon the risk of over-moderation, that is to say the reflex to delete content simply for safety reasons in order to avoid any kind of liability. They also recalled

---

<sup>362</sup> <https://algorithmwatch.org/en/automated-moderation-perspective-bias/>.



that freedom of expression must be ensured in combination with the right to receive information, so that everyone can form their opinion on the basis of correct information.

Representatives of social media services stressed that freedom of expression is an essential component of their service, although at the same time it must be balanced with the need to ensure a certain level of integrity and safety within the platform, hence the creation by some of "community standards". These are intended to be applied globally but must also take account of local contexts and legal frameworks. In addition, they must be both clear enough to allow rapid decision-making with a good degree of certainty, but also durable enough to stand the test of time and changing social norms. Representatives from the field of trust and online security also echoed this challenge of how to find standards that embody the right kind of values to uphold and that remain independent of political power.

Another purpose of these standards is to get closer to the issues addressed by the DSA Package, which are to ensure more accountability, transparency, and oversight over online platforms and their activities. Regarding the "Europeanised" version of the Good Samaritan clause, the representatives of social media explained that it constitutes a step in the right direction as it allows for these proactive measures to be taken without automatic loss of exemption from liability. With regard to the new transparency requirements, the representatives stressed that there are different degrees of transparency and that these requirements do not necessarily lead to a breach of trade secrets but do imply real structural changes in companies. Representatives of media NRAs for their part added that this transparency was essential in order to ensure their tasks of supervision can be carried out and may require the intervention of third parties to verify the veracity of the data provided by the platforms.

### **8.3. Webinar #2 - Gatekeepers in the DSA Package: What about VoD?<sup>363</sup>**

#### **8.3.1. Setting the scene**

Gilles Fontaine, Head of the Department for Market Information at the European Audiovisual Observatory, kicked off the webinar by sharing some insights on the VoD sector and its place in the European audiovisual ecosystem. VoD markets are characterised by three types of business model: TVOD, with title-based transaction fees; SVOD, with monthly subscription; and AVOD, which relies on advertising. The distinction between these services is not always clear. For example, some broadcasters often make offers that include access to both linear channels and on-demand content, all within a single subscription. Regarding

---

<sup>363</sup> This section briefly summarises the discussions from the second webinar "Gatekeepers in the DSA Package: What about VoD?", 22 April 2011, <https://www.obs.coe.int/en/web/observatoire/-/series-of-webinars-from-march-to-july>. The summary reflects only the main points of the discussions, so please check upon delivery: the recording of the conference is available at <https://youtu.be/hlhMwtYQjnU>.

the distribution models, four main models can be distinguished: full over-the-top services (auto-distributed); services distributed by a pay-TV packager (e.g., IPTV operator) and where this pay-TV packager retains the customer relationship; services referenced by a cable or IPTV operator, in which case it is the VoD service which retains the subscriber relationship; and services operated by the cable or IPTV operators themselves.

In terms of market data, the figures that are available show that SVOD is the fastest-growing segment and is starting to be significant compared to pay TV, while TVOD is still growing but has not yet reached maturity level. Finally, regarding the main players active on these different markets, at European level, international services share the lion's share of the market while, at national level, national players can sometimes rank in the top 3.

### 8.3.2. The expert's corner: Regulatory and competition-related aspects

Oliver Budzinski, Professor of Economic Theory (Chair) at Ilmenau University of Technology, addressed the issue of competition in the VoD market. According to most economic theories, effective competition can prevent gatekeeping. In the VoD markets, there is currently a lot of competition between SVOD services, but also with AVOD services (such as YouTube) and with linear television. The expert then explained in more detail the different elements that create a gatekeeper and how they can be translated into the VoD markets: network effects related to platforms; the data-driven business model; the emergence of a one-stop shop on the consumer side; and vertical integration at all stages of the market. For the time being, VoD services show characteristics that can only partly be related to the first three elements as such.

However, vertical integration can already be seen with some of the major VoD services such as Disney+, Netflix, or Amazon, which produce and distribute content via the Internet to consumers' homes. The combination of this vertical integration, with an offer responding to consumers' desire for a one-stop shop, and the use of personalised data, in particular via algorithmic search and recommendation systems, may in fact lead to gatekeeper effects, barriers for smaller production companies to enter the market, and self-preferencing, in other words the re-orientation of the audience towards their own content. Furthermore, the expert pointed out that in modern economic theory, dominance of the relevant market is not necessary for these effects: size and exceptional relevance in the market, in a given ecosystem, are sufficient. As a conclusion, big and vertically integrated players can be gatekeepers without dominating the market.

### 8.3.3. The stakeholders' panel: The VoD market, a competitive and heavy regulated market without gatekeepers?

Representatives of the European Commission started the discussion by explaining that VoD services were excluded from the scope of the DSA Package as the VoD market is already



heavily regulated, and also because the DSA serves a different purpose and focuses on creating a strong liability framework to protect users and establish a graduated level of liability for online platforms, which covers some new players in media regulation at EU level, such as video-sharing platforms like YouTube or Facebook, but not VoD services. Furthermore, they were also not included in the scope of the definition of gatekeepers under the DMA because they do not share the typical characteristics of multilateral markets, nor the network effects of traditional gatekeepers in the meaning of the proposal. This can be explained by the high cost of producing audiovisual content for the VoD services, while the switching costs are not particularly high for users. In addition, the VoD market is a very dynamic and competitive market, where new players can still appear. Moreover, the DMA focuses mainly on gatekeepers operating in a market with a high level of concentration and high barriers to entry, which is not the case for most VoD services, and VoD services behaving as gatekeepers might still be included and considered as such in the future through Article 17 of the DMA following a market investigation.

Moreover, it was recognised, notably in the Media and Audiovisual Action Plan (MAAP),<sup>364</sup> that certain negative trends are emerging, such as application of the “work-for-hire” model to European authors and producers, which may lead to a lock-in of talents and producers within a certain platform. The author representatives deplored the fact that, despite this recognition, no appropriate remedy has been proposed in the MAAP and DSA package. They shared their concern about this new trend, which risks depriving European audiovisual authors of their intellectual property rights. Several participants highlighted the fact that the VoD sector was already a heavily regulated sector at the EU level and justified their exclusion with the *lex specialis* approach. In particular, some pointed out that under the AVMS Directive they already have full editorial responsibility and accountability, and this responsibility would have been reduced if they had been included in the DSA. Others argued that the DSA aimed at filling in a legislative gap by regulating online intermediaries, whereas VoD services are already regulated. More specifically, the representatives of commercial broadcasters and VoD services underlined that the VoD market, despite its complexities, is a younger market than the one the DMA seeks to address and the entry of big streamers, such as Disney + last year, did not result in lock-in effects or barriers to other competitors. For their part, representatives of telecommunications services explained that for them it wouldn’t make sense to have two parallel competition regimes since, as a telecoms operator providing linear and non-linear services, they are already regulated as a pay-TV provider but also as a VoD services provider. The VoD markets together with the pay-TV market are a very commercially competitive field for content distribution all across Europe.

On the other hand, several participants argued that some VoD services could fit the qualification of “gatekeepers”. Representatives of authors expressed some difficulty with the bundled offerings of very large platforms that could fit the qualification of gatekeepers, such as Amazon and its Amazon Prime offering, as these bundled offers make it difficult for the collective management organisations of audiovisual authors to define a tariff based on the revenues generated by the VoD services. On the side of independent producers, some

---

<sup>364</sup> [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_2239](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2239).



denounced the fact that certain VoD services are currently behaving, or may in the very near future behave, as gatekeepers within the meaning of Article 3 of the DMA.

In addition, most participants agreed on the need for greater transparency. Representatives of authors expressed the need to develop some kind of company or tool for measuring the performance of a work on VoD platforms, similar to that which already exists for the film and broadcasting sector. Independent producers deplored the fact that the DMA's transparency obligations do not also apply to VoD services and called for more transparency on the data and algorithms used by the major streamers, which would allow them to obtain valuable information on audience performance data or on the functioning of personalised recommendation algorithms. Representatives of the smaller VoD platforms testified that sharing data with consumers and getting feedback on their interests helps them to provide better products and services in the long run. They also said that it can be difficult to get data on algorithms, but that nevertheless this is something they are committed to improving over time.

## 8.4. Webinar #3 - Copyright and the digital services act<sup>365</sup>

### 8.4.1. Setting the scene

Maja Cappello, Head of the Department for Legal Information at the European Audiovisual Observatory, started the webinar on the issue of copyright within the DSA. She briefly presented the main types of measures introduced by the DSA to help fight illegal content online, such as: the “trusted flaggers” cooperation mechanisms for users to flag illegal content; and the KYBC principle, which consists of rules on traceability of business users in online marketplaces, to detect sellers of illegal goods. The DSA also harmonises due diligence obligations for platforms and hosting services and aims at helping member states enforce the law online, by establishing mechanisms for issuing orders to service providers throughout the Single Market.

Among the possible types of illegal content is the unauthorised distribution of copyrighted content, and the DSA presents several points of contact with current copyright rules, as defined in the DSM Directive. Article 17 of this Directive, the application of which is (at the time of the webinar) still to be clarified by Commission guidelines and which is currently the subject of a case pending before the CJEU, makes online content-sharing platforms (OCSPs) directly liable if their users upload unauthorised copyright-protected works or subject matters on their platforms under certain conditions. The discussion held during this webinar helped shed light on the new rules of the DSA in relation to copyright, and in parallel to the DSM directive.

---

<sup>365</sup> This section briefly summarises the discussions from the third webinar “Copyright and the DSA”, 27 May 2011, <https://www.obs.coe.int/en/web/observatoire/-/series-of-webinars-from-march-to-july>. The summary reflects only the main points of the discussions, so please check upon delivery: the recording of the conference is available at [https://youtu.be/BHGvv2UJ\\_OU](https://youtu.be/BHGvv2UJ_OU).



## 8.4.2. The experts' corner: Risks and opportunities of the DSA

Eleonora Rosati, Professor of IP Law of Stockholm University and Director of the Institute for Intellectual Property and Market Law (IFIM) opened by discussing the various risks and opportunities of the DSA in relation to copyright protection. She underlined that the histories of the DSA and the DSM Directive are closely intertwined, although there is no formal relationship between these two instruments, with the principle of *lex specialis* and the provisions of Article 1 of the DSA providing that it is without prejudice to the rules laid down by Union law on copyright and related rights.

The expert then explained in detail the specific and complex liability regime foreseen by Article 17 of the DSM Directive, which is premised on a basic idea that online content-sharing service providers (OCSSP) perform certain acts of communication to the public of copyright-protected content, for which they have to secure the authorisation of relevant rightsholders. However, this article also envisages a special liability mechanism in the event that the OCSSP has made best efforts to secure such authorisation but failed to obtain one: the provision shields them from liability provided that a series of cumulative requirements is fulfilled, which ensure a form of minimum assistance and protection to rightsholders. The DSM Directive also provides for a restatement that the provision should not entail a general monitoring obligation which mirrors Article 15 of the e-Commerce Directive.

Concerning the interplay and similarity between these two instruments, the DSA contains several provisions that will serve application of Article 17 of the DSM Directive. For instance, while the DSM Directive does not specify the territorial conditions under which an OCSSP will be caught within Article 17, the DSA adopts a targeting approach. The DSA contains calculation methods to determine the number of unique monthly visitors of the OCSSP, which in turn will be relevant to determine the application of the softer liability regime foreseen by Article 17. Moreover, it provides a regulation-of-trusted-flaggers system, which for some commentators could be necessary to make Article 17 workable. It is therefore important to monitor the development of these two instruments.

## 8.4.3. The stakeholders' panel: Interplay between the DSA and copyright, risks, challenges, and opportunities

The representatives of the European Commission set the scene by explaining their views on the interaction between the DSA and copyright protection. The DSA is a horizontal instrument designed to govern a number of important aspects of the Internet economy, not specifically the issue of copyright. This rule, which derived in particular from Article 1 of the DSA, reflects the political intention to not reopen the DSM Directive to the DSA negotiations. This means that online platforms dealing with copyright-protected content are not covered by the liability regime of the DSA, but by the specific regime of the DSM Directive, as set up in particular by its Article 17. In the same spirit, representatives of the online platforms recalled that the drafting and implementation process of the DSM



Directive was the result of a very complex and long negotiation and cautioned against trying to change some elements of it.

Representatives of the creative sector discussed the impact of the DSA on the fight against illegal content, from the perspective of cybercriminal activities. In their view, the “Good Samaritan” clause and the due diligence obligations as provided for in the DSA do not really constitute a major change in the fight against online piracy. They also considered that these obligations should be strengthened, or at least that compliance with them should be a condition for benefiting from liability exemption. The KYBC obligations are particularly constraining for cyber criminals as they oblige them to provide true and verifiable contact information when signing up for web hosting or domain names. However, these are limited to the e-commerce marketplaces.<sup>366</sup> Representatives of authors also criticised this limited scope and recommended that it should be extended to all types of online intermediaries in order to tackle illegal content and repeat infringement efficiently in the digital environment. For authors, these obligations constitute an important tool to identify infringers and illegal content and help ensure that private copying compensation is not circumvented online.

Representatives of platforms expressed some concerns regarding the implementation process of certain elements of the Directive, such as the principle of best efforts under Article 17, and how this would be defined by the different member states. Here, the DSA provides some clarity and guidance for representatives of platforms as to the extent of their liability and obligations, such as for instance the description of notice. On the same issue of clarity, representatives of viewers deplored the lack of detail of some of the DSA provisions. In their view, there is a great deal at stake in how these provisions will be transposed, and how they will be clarified and interpreted by future Commission guidelines and the case law of the CJEU. It is therefore imperative that the transparency and accountability obligations for instance are fulfilled and explained in plain and clear language, as this will strengthen trust in the legal framework. These transparency requirements were welcomed by representatives of authors as transparency is paramount to visibility regarding infringements which helps better prevent illegal content online, and also provide authors with essential information about the exploitation of their works, hence allowing them to evaluate remuneration rates during contractual negotiations.

On the perspective of users’ rights, representatives of viewers welcomed some positive elements of the DSA package, such as the fact that it makes more references to fundamental rights, compared to other pieces of EU legislation, and the potential to significantly improve the transparency and accountability of decisions made by Internet intermediaries to remove or otherwise restrict access to content. Regarding the risks for users’ rights, they concern primarily the impact of the proposed measures upon fundamental rights, in particular freedom of expression and the rights to privacy and data protection. The risk of over-blocking with a sort of “privatisation” of online content regulation was also highlighted, as technological tools are not effective in assessing the context in which content is posted online, making it impossible to distinguish copyright infringements from legal uses of protected content. In addition, user representatives believe that the current liability exemption regime incentivises platforms to avoid liability

---

<sup>366</sup> For more information on that subject, please visit the following website: <https://www.kybc.eu/>.



by over-blocking content in case of ambiguity and that the safeguards against this risk are not sufficiently defined by the DSA. Regarding the liability regime, representatives of the creative sector went further and deplored the fact that the loss of the liability exemption is conditional on proof of deliberate collaboration between the provider of intermediary services and the recipient of those services with regard to the undertaking of illegal activities.

## 8.5. Webinar #4 - The Digital Services Act and the fight against disinformation<sup>367</sup>

### 8.5.1. Setting the scene

Maja Cappello, Head of the Department for Legal Information at the European Audiovisual Observatory, introduced the subject of this last webinar on the role of the DSA in the wider ecosystem of codes and actions related to the fight against disinformation. Several initiatives have already been developed by the European Commission, such as the Communication on “Tackling online disinformation: A European approach”,<sup>368</sup> the Action Plan on Disinformation<sup>369</sup> and the Code of Practice on Disinformation.<sup>370</sup> The DSA proposal establishes now a co-regulatory safety net for the measures that will be included in a revised and strengthened Code. It even contains provisions concerning the set-up of codes of conduct at EU level under Article 35 of the DSA, considering the specific challenges of tackling different types of illegal content and systemic risks as those connected to disinformation via Article 26 of the DSA.

### 8.5.2. The expert’s corner: Risks and opportunities for the fight against disinformation

Tarlach McGonagle, Associate Professor at the Institute for Information Law (IViR) of the University of Amsterdam and Professor of Media Law and Information Society at the University of Leiden, presented how the European institutions have dealt with the issue of disinformation and the various successive definitions that have been developed for this

---

<sup>367</sup> This section briefly summarises the discussions from the fourth webinar “The DSA and the fight against disinformation”, 1 July 2011, <https://www.obs.coe.int/en/web/observatoire/-/series-of-webinars-from-march-to-july>. The summary reflects only the main points of the discussions, so please check upon delivery: the recording of the conference is available at <https://youtu.be/bPj4ZSA3IEQ>.

<sup>368</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236>.

<sup>369</sup> <https://digital-strategy.ec.europa.eu/en/library/action-plan-against-disinformation>.

<sup>370</sup> <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>.



concept. A first report commissioned by the Council of Europe<sup>371</sup> provided some elements of definitions. A subsequent definition was then developed from the 2018 Code of Practice and other EU instruments, which defined disinformation as verifiably false or misleading information that is created, presented and disseminated for economic purposes or to intentionally mislead the public and which may cause public damage intended to threaten democratic political and policy-making processes and public goods such as the protection of the health of EU citizens or security.<sup>372</sup>

Other European texts and tools, including the European Democratic Action Plan,<sup>373</sup> have brought more clarity and refinement to these definitions, giving more details on how disinformation is disseminated, from whom it is originated, and the different types of harm it can cause. Regarding the actors involved in the creation and dissemination, the expert underlined the importance of being clear-sighted in differentiating between them and the complexity of their role. Moreover, to deal effectively with this kind of disinformation there need to be important regulatory approaches on the one hand, and investment in the ecosystem as such on the other hand, to put in place measures and structures that will ensure that the framework for freedom of expression is robust and resilient. Some key elements of the DSA, such as the risk assessment and mitigation regime foreseen by its Articles 25-27, are particularly important, especially for the very large online platforms, given the wide reach they offer, which implies in parallel a wider potential impact of disinformation spread. However, the expert cautioned against this leading up to blind spots for other actors where the dissemination of this information can take place in a very intense and effective way.

### 8.5.3. The stakeholders' panel: Tackling disinformation, freedom of expression and access to data

Representatives of the European Commission presented their policy and recent initiatives in tackling disinformation. A recent Eurobarometer survey<sup>374</sup> shows that online disinformation is a significant and growing concern for European citizens, and this concern has been accentuated with the Covid-19 crisis. In this context, the Commission has put in place a Covid-19 disinformation-monitoring programme on the online platforms that are signatories of the Code of Practice. The findings of this monitoring programme were used by the European Commission to produce guidance<sup>375</sup> aimed not only at strengthening the Code, but also at bridging the legislative gap while waiting for the DSA's adoption and

---

<sup>371</sup>Wardle C. And Derakhshan H., "Information disorder: Toward an interdisciplinary framework for research and policy making", 2017, <https://edoc.coe.int/fr/medias/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html>.

<sup>372</sup> For more information, visit the website of the Commission:

<https://digital-strategy.ec.europa.eu/en/policies/online-disinformation>.

<sup>373</sup> [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_20\\_2250](https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2250).

<sup>374</sup> <https://ec.europa.eu/digital-single-market/en/news/final-results-eurobarometer-fake-news-and-online-disinformation>.

<sup>375</sup> Guidance to strengthen the Code of Practice on Disinformation, May 2021,

[https://ec.europa.eu/commission/presscorner/detail/en/OANDA\\_21\\_2586](https://ec.europa.eu/commission/presscorner/detail/en/OANDA_21_2586).



ensuring greater transparency in political advertising. Several panellists expressed satisfaction with the guidance, including representatives of commercial broadcasters who commented that, in their view, it responded to a growing call for monitoring of the code based on key performance indicators, as well as a recognition of the importance of advertising transparency and the commitment to a co-regulatory system. Representatives of commercial broadcasters did, however, outline a few elements that could be strengthened. For example, they suggested there should be more transparency on verifiability actions by media NRAs, stressed that independent audits should be high on the list of other DSA commitments to be included in the revised code, and called for stronger sanction mechanisms.

Other current challenges and risks linked to fact-checking activities and disinformation were addressed. Representatives of the Commission mentioned that studies have shown that the efficiency of the measures put in place by platforms depends on the language of the content concerned.<sup>376</sup> Others deplored the fact that some fact checkers do not receive bulk data. Representatives of users also stressed the dissemination of disinformation being influenced by the algorithms and recommendation systems in place, and that users can be unaware of this risk of receiving information biased by the information they have previously looked for. Moreover, several participants underlined the growing importance of disinformation and its particularly harmful effect in recent years. However, some participants also warned against the risk of restricting freedom of expression, stressing online expression is entitled to protection under international human rights law irrespective of whether it is true or false. Only certain categories of speech, such as incitement to hatred, should be restricted. Others cautioned, in particular, regarding the difficulties of disentangling untrue facts from opinions and determining who should be responsible for identifying between the two. It is also important to note that misinformation represents only a small part of the information available and fighting against it should not lead to the takedown of legitimate speech. In this regard the representatives of the Commission mentioned that the Code of Practice on Disinformation and the Guidance are fully grounded in the protection of freedom of expression. Notably, they contain exactly for this reason a wide variety of tools to fight disinformation, out of which none is about takedown. In addition, the Guidance asks for transparency and appropriate redress mechanisms regarding actions taken regarding content that allegedly contains disinformation. On the issue of access to data, representatives of commercial broadcasters called for online platforms to commit to independent audits, in order to effectively verify the monitoring results. For their part, online platforms underlined the need to have some sort of safeguard to ensure respect for trade secrets which would make such data accessible, and in these conditions, potential allow independent audits. On that note, some participants noted the need for care regarding how audits are conducted and by whom.

In conclusion, the representatives of the Commission mentioned that the Code of Practice would, through the combination of Articles 26 and 35 of the DSA, be elevated to the status of a co-regulatory system, a code of conduct to which online platforms could adhere and be part of, in particular when fulfilling the obligation to assess and mitigate risks. Strengthening the commitments, increasing the number of signatories, encouraging strong cooperation between these actors, and demonetising disinformation are key steps

---

<sup>376</sup> [https://secure.avaaz.org/campaign/en/facebook\\_neglect\\_europe\\_infodemic/](https://secure.avaaz.org/campaign/en/facebook_neglect_europe_infodemic/).



to be taken in order to make this code more effective and the fight against disinformation more efficient. Other participants pointed out that an important response to disinformation is also to ensure a constant flow of high quality and diverse sources of information. In this sense, media literacy programs, but also funding for independent media and fact-checking activities, are fundamental. Representatives of the European Digital Media Observatory (EDMO),<sup>377</sup> established within the EC strategy to tackle online disinformation, underlined the role of this organisation as a centralised independent platform that gathers stakeholders and provides relevant facts and tools which help ensure the multidisciplinary and evidence-based approach in tackling disinformation online. Representatives of platforms indicated that this multi-stakeholder approach was, from their experience, a more efficient way to tackle disinformation and that they relied heavily on the role of EDMO in bringing stakeholders together.

## 8.6. List of participants

	Surname	Name	Organisation	Position
1	Barata	Joan	Stanford Law School	Intermediary Liability Fellow
2	Budzinski	Oliver	Ilmenau University of Technology	Director of the Institute of Economics
3	Burnley	Richard	European Broadcasting Union (EBU)	Director of Legal and Policy/General Counsel
4	Celot	Paolo	EAVI	Secretary General
5	Cole	Mark	European Media Law (EMR)	Director for Academic Affairs
6	Craig	Celene	Broadcasting Authority of Ireland (BAI)	Deputy Chief Executive
7	De Streel	Alexandre	University of Namur	Academic Co-director at CERRE
8	Despringre	Cécile	Society of Audiovisual Authors (SAA)	Executive Director
9	Durand-Vialle	Pauline	Federation of European Screen Directors (FERA)	Chief Executive
10	El Ramly	Siada	Dot Europe	Director General

---

<sup>377</sup> <https://edmo.eu/>



	Surname	Name	Organisation	Position
11	Estrin	Miriam	Google	Policy Manager
12	Giorello	Marco	European Commission (DG CONNECT)	Head of Unit for Copyright
13	Gori	Paula	EDMO	Secretary-General and Coordinator
14	Herold	Anna	European Commission (DG CONNECT)	Head of the Audiovisual and Media Policy Unit
15	Herovanu	Miruna	Association of Commercial Television in Europe (ACT)	Senior EU Affairs officer
16	Jiménez Martín	Marisa	Facebook	Director Public Policy and Deputy Head of EU Affairs
17	Kukliš	Ľuboš	Council for Broadcasting and Retransmission of Slovakia	CEO
18	Lebret	Alexandra	European Producers Club (EPC)	Managing Director
19	Martin	Stéphanie	Society of Audiovisual Authors (SAA)	Legal Advisor
20	McCoy	Stan	Motion Picture Association (MPA)	President and Managing Director (EMEA)
21	McGonagle	Tarlach	Institute for Information Law (IViR)	Associate professor
22	Michalis	Maria	European Alliance of Listeners' and Viewers' Associations (Euralva)	European audiovisual policy adviser
23	Morrow	Paige	UN Special Rapporteur for Freedom of Opinion and Expression	Legal Advisor
24	Pancini	Marco	YouTube	Director Public Policy EMEA
25	Polad	Grégoire	Association of Commercial television in Europe (ACT)	Director General
26	Putman	Marc	EUROVOD and OUTTV	President and CEO
27	Rosati	Eleonora	Institute for Intellectual Property and Market Law (IFIM), Stockholm University	Professor of Intellectual Property Law and Director



	<b>Surname</b>	<b>Name</b>	<b>Organisation</b>	<b>Position</b>
<b>28</b>	Senftleben	Martin	University of Amsterdam	Director of IViR
<b>29</b>	Solar-Bassett	Anna	Vodafone	Group Public Policy
<b>30</b>	Stump	Krisztina	European Commission (DG CONNECT)	Head of the Media Convergence and Social Media Unit
<b>31</b>	Willner	Charlotte	Trust & Safety Professional Association (TSPA/TSF)	Executive Director

### European Audiovisual Observatory

	<b>Name</b>	<b>Surname</b>	<b>Position</b>
<b>1</b>	Nikoltchev	Susanne	Executive Director
<b>2</b>	Cabrera Blázquez	Francisco Javier	Senior Legal Analyst - Department for Legal Information
<b>3</b>	Cappello	Maja	Head of Department for Legal Information
<b>4</b>	Hindhaugh	Alison	Communications Manager
<b>5</b>	Talavera Milla	Julio	Analyst - Department for Legal Information
<b>6</b>	Valais	Sophie	Senior Legal Analyst - Department for Legal Information
<b>7</b>	Chochon	Léa	Junior analyst - Department for Legal Information
<b>8</b>	Rabie	Ismail	Junior analyst - Department for Legal Information





A publication  
of the European Audiovisual Observatory

