



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

DOTTORATO DI RICERCA IN

DIRITTO EUROPEO

Ciclo 38

Settore Concorsuale: 12/E4 - DIRITTO DELL'UNIONE EUROPEA

Settore Scientifico Disciplinare: IUS/14 - DIRITTO DELL'UNIONE EUROPEA

COUNTERBALANCING DIGITAL PLATFORMS' OPINION POWER: THE
DIGITAL SERVICES ACT AND COMPLEMENTARY REGULATIONS

Presentata da: Anna Vicinanza

Coordinatore Dottorato

Giacomo Di Federico

Supervisore

Pietro Manzini

Co-supervisore

Giacomo Di Federico

Esame finale anno 2026

COUNTERBALANCING DIGITAL PLATFORMS' OPINION POWER: THE *DIGITAL SERVICES ACT* AND COMPLEMENTARY REGULATIONS

TABLE OF CONTENTS

INTRODUCTION	6
I. DIGITAL PLATFORMS AS INFORMATION GATEKEEPERS: OPINION POWER IN THE DIGITAL REALM.....	16
1. A PLATFORM ECONOMY AND INTERMEDIATED ACCESS TO INFORMATION.....	17
1.1. <i>A Highly Concentrated Digital Economy: Big Tech's Dominance in Economic and Social Interactions</i>	<i>18</i>
1.2. <i>Gatekeeping Politically Relevant Information: Opinion Power of Social Media Platforms and Search Engines</i>	<i>22</i>
2. PLATFORMS' OPINION POWER AND THE PUBLIC INTEREST.....	30
2.1. <i>Moderation and Prioritisation: Content Curation Practices by the Gatekeeper</i>	<i>31</i>
2.2. <i>Extending Public Interest Regulation to New Information Intermediaries</i>	<i>41</i>
CONCLUDING REMARKS	46
II. INTERMEDIARIES' LIABILITY FOR THIRD-PARTY ILLEGAL CONTENT AND DUTIES TO ACT	49
1. FROM SAFE HARBOUR TO DEMANDS FOR ACCOUNTABILITY	50
1.1. <i>Safe Harbour: Intermediaries' Liability Exemptions in the US and EU Legal Systems</i>	<i>51</i>
1.2. <i>Questioning Safe Harbour: Are Online Platforms Mere Intermediaries?</i>	<i>58</i>
1.3. <i>Towards an Enhanced Responsibility of Online Platforms within the EU.....</i>	<i>69</i>
2. THE LIABILITY REGIME FOR ONLINE PLATFORMS AND MANDATORY MODERATION ACTIVITIES UNDER THE DSA	72
2.1. <i>Scope of the DSA: the Escalating Obligations System</i>	<i>75</i>
2.2. <i>The Good Samaritan Protection and Reporting Obligations</i>	<i>78</i>
2.3. <i>'Awareness' of Illegality and Notice-and-Action Mechanisms.....</i>	<i>80</i>
Injunctions and information requests by national authorities	81
Reporting mechanisms accessible by users and trusted flaggers	84

Measures against abusive conducts by users	88
2.4. VLOPs and VLOSEs Special Accountability for Illegal and Harmful Content..	89
Designation of VLOPs and VLOSEs by the European Commission	89
Systemic risks assessment and mitigation measures: a new obligation to moderate content?	92
Code of conducts and the crisis response mechanism	98
CONCLUDING REMARKS	100
III. MODERATION ACTIVITIES: THE DSA FRAMING CONTENT RESTRICTIONS	104
1. THE DSA'S FRAMEWORK ON MODERATION ACTIVITIES	112
1.1. <i>Transparency Obligations on Moderation Activities</i>	114
Transparency of terms and conditions on moderation policies.....	114
Transparency reports on moderation activities	116
1.2. <i>Due Process Obligations for Content Restrictions: Statement of Reasons and Redress Mechanisms</i>	118
The obligation to state reasons when applying restrictions on content	119
Accessibility to redress mechanisms against decisions on restrictions and the right to human review.....	121
1.3. <i>The Need to Respect Fundamental Rights in Moderation Activities</i>	127
Fundamental rights and terms of service	128
Fundamental rights and moderation activities in the systemic risks assessment for VLOPs and VLOSEs	130
2. CONTENT RESTRICTIONS TOWARDS MEDIA ENTITIES ON VLOPs: THE SPECIAL EMFA'S REGIME	132
2.1. <i>Scope of the Media Freedom Act: the Definition of 'Media Service'</i>	134
2.2. <i>A 'Media Privilege' on VLOPs</i>	137
CONCLUDING REMARKS	142
IV. PRIORITISATION, RANKING, AND RECOMMENDER SYSTEMS	146
1. THE DSA REGULATING RECOMMENDER SYSTEMS	152
1.1. <i>Transparency Obligations on Recommender System: a Right to Explanation?</i>	153
General transparency obligations for recommender systems	153
Transparency obligations for online advertisement	156
1.2. <i>Restrictions on Targeted Recommendations</i>	159
Restrictions on profiling practices for the purposes of online ads	159

Right to an option of recommender systems not based on profiling	163
1.3. <i>Systemic Risks Assessment on Recommender Systems</i>	165
2. THE DMA RESTRICTIONS ON THE USE OF DATA AND THEIR IMPACT ON RECOMMENDER SYSTEMS	168
2.1. <i>Gatekeepers vs. VLOPs and VLOSEs</i>	169
2.2. <i>Restrictions on the Utilisation of User Data</i>	171
The prohibition of combining personal data without user consent	171
Meta ‘pay-or-consent’ model and subsequent developments	175
3. THE REGULATION ON POLITICAL ADVERTISING	180
3.1. <i>The Problem of Defining Political Speech</i>	181
3.2. <i>Lawful Targeted Political Advertisement: Explicit Consent and Restrictions on Profiling</i>	184
Explicit and separate consent for targeted political advertising	185
The prohibition of profiling based on sensitive data for targeted political advertising	186
3.3. <i>Transparency Obligations on Political Advertising for Online Platforms</i>	187
CONCLUDING REMARKS	190

V. AN HOLISTIC PERSPECTIVE ON DIGITAL PLATFORM REGULATION: CHALLENGES FOR EFFECTIVE OVERSIGHT AND ENFORCEMENT 195

1. TECHNOLOGICAL INTERSECTIONS AND REGULATORY OVERLAPS	206
2. THE FRAGMENTED ENFORCEMENT STRUCTURE OF PLATFORM REGULATION.....	210
2.1. <i>National Authorities Enforcing Regulations on Digital Platforms</i>	214
Multiple national authorities enforcing the same regulation	214
Multiple national authorities enforcing overlapping regulations.....	215
2.2. <i>Transnational Coordination in a Fragmented Enforcement Landscape</i>	218
Transnational enforcement under a single framework.....	218
Transnational enforcement from a cross-framework perspective.....	220
2.3. <i>Supranational Enforcement of Digital Platforms Regulations</i>	221
Vertical relationships in the enforcement structure	222
Vertical relationships under a single framework	222
Vertical relationships from a cross-framework perspective	223
Horizontal relationships in supra-national enforcement	225
Horizontal relationships within a single framework	226
Horizontal relationships from a cross-framework perspective.....	226
CONCLUDING REMARKS	228

CONCLUSIONS.....	231
BIBLIOGRAPHY.....	238
CASE-LAW.....	266
APPENDIX.....	268

INTRODUCTION

We live in an age of extremely diffused speech, but concentrated distribution.¹ On the one side, the web has expanded opportunities for content production, amplifying the potential variety of information sources.² On the other, online information transmission is systematically intermediated by a limited number of platform services.³ Intermediation comes with a specific form of power, i.e. gatekeeping, allowing few dominant intermediaries to globally structure the rules of information transmission.⁴ This includes the possibility to deny access to their services, a practice that can be broadly labelled as *moderation*, as well as the ability to influence the actual dissemination of content, referred to as *prioritisation*.

This concentration in distribution channels is effectively conveyed by Tim Wu's metaphor of the 'master switch': '*Google is the Internet's switch. In fact, it's the world most popular Internet switch, and as such, it might even be described as the current custodian of the Master Switch*'.⁵ The metaphor underlines that in a digital platform economy, when the most widely used intermediary demotes, de-indexes, or excludes certain content from search results, its visibility is severely diminished, to the extent that, it may effectively vanish from the global public sphere. Conversely, when it chooses to turn the light on a particular piece of information, it is suddenly illuminated before a global audience.

¹ Tim Wu, 'Is Filtering Censorship? The Second Free Speech Tradition' (*Brooking.edu*, 27 December 2010) 12 <<https://www.brookings.edu/articles/is-filtering-censorship-the-second-free-speech-tradition/>> accessed 13 November 2024.

² Jürgen Habermas, *Nuovo mutamento della sfera pubblica e politica deliberativa* (Raffaello Cortina Editore 2023) 46; Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology' [2023] Faculty Books Introduction <<https://scholarship.law.columbia.edu/books/367>>.

³ Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019) 41.

⁴ Cohen (n 3) 45; Natali Helberger, Katharina Kleinen-von Königslöw and Rob Noll, 'Regulating the New Information Intermediaries as Gatekeepers of Information Diversity' (2015) 17 *Info* 50, 50, 57.

⁵ Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Faculty Books 2010) 282 <<https://scholarship.law.columbia.edu/books/176>>.

When analysing such gatekeeping power in the context of politically relevant information, it translates into opinion power, which can be defined as the capacity to select certain content for the exposure to a large audience.⁶ In the media sector, the opinion power of distributors has traditionally attracted regulatory attention,⁷ precisely because of their bottleneck position between content producers and the audience. Yet, technological innovation has altered the infrastructure of distribution, requiring a rethinking of preexisting solutions,⁸ adapting them for the digital space.

Due to their crucial role in contemporary social and economic life, digital platforms have become the primary focus of several key initiatives within the EU Digital Strategy,⁹ together with developers and deployers of AI systems. The adoption of these regulatory instruments marked Europe's '*constitutional moment*' for the

⁶ Natali Helberger and others, 'Dealing with Opinion Power in the Platform World: Why We Really Have to Rethink Media Concentration Law' (2023) 11 Digital Journalism 1542 <<https://doi.org/10.1080/21670811.2022.2161924>> accessed 13 November 2024.

⁷ Wu, 'Is Filtering Censorship? The Second Free Speech Tradition' (n 1); Martin Moore, *Tech Giants and Civic Power* (CMCP, Policy Institute, King's College London 2016) 29; Philip Napoli, *Social Media and the Public Interest. Media Regulation in the Disinformation Age* (Columbia University Press 2019) 59 <<https://cup.columbia.edu/book/social-media-and-the-public-interest/9780231184540>> accessed 13 November 2024; Frank Pasquale, 'Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power' (2016) No. 2016-24 University of Maryland Francis King Carey School of Law <<https://papers.ssrn.com/abstract=2779270>> accessed 13 November 2024; Damian Tambini, 'Social Media Power and Election Legitimacy' in Damian Tambini and Martin Moore, *Digital Dominance. The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018).

⁸ Moore (n 7) 30.

⁹ Ursula von der Leyen, 'A Union That Strives for More. My Agenda for Europe. Political Guidelines for the next European Commission 2019-2024' <https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en?filename=political-guidelines-next-commission_en.pdf>. See also: 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; Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the *European Democracy Action Plan*, 3.12.2020, COM/2020/790/final.

digital sphere,¹⁰ a momentum that however now appears to be fading under a renewed push for deregulation.¹¹

The Digital Services Act, in particular, constitutes the EU's most ambitious attempt to regulate online platforms to date, representing a horizontal framework for all digital intermediaries, with specific and enhanced obligations for major platforms. Its aim is to enhance democratic control over the platform ecosystem, rebalancing the relationships between users, platforms, and public authorities in accordance with European values and, therefore, placing citizens at the centre.¹² It broadly ensures greater accountability for how platforms moderate content, manage advertising and design their algorithmic systems. While the Digital Services Act stands as a reference point on these issues, it is complemented by other regulations. The European Democracy Action Plan, for instance, also called for rules on the transparency of sponsored political content, later enshrined in the Regulation on the Transparency and Targeting of Political Advertising,¹³ as well as for measures to strengthen media freedom and pluralism, which led to the adoption of the European Media Freedom Act.¹⁴ Moreover, the Digital Markets Act (DMA)¹⁵ complements

¹⁰ Anu Bradford, 'Europe's Digital Constitution' [2023] Verfassungsblog <<https://verfassungsblog.de/europes-digital-constitution/>> accessed 23 September 2025.

¹¹ Eddy Wax, 'EU Tech Laws Imperilled by Friend and Foe' (*Euractiv*, 27 August 2025) <<https://www.euractiv.com/section/politics/news/eu-tech-law-imperilled-friend-for-capitals/>> accessed 27 August 2025; Oreste Pollicino, 'Rights-Proof Simplification: The DigCon Project's Contribution to the EU's Digital Omnibus Consultation' (*MediaLaws*, 17 October 2025) <<https://www.medialaws.eu/rights-proof-simplification-the-digcon-projects-contribution-to-the-eus-digital-omnibus-consultation/>> accessed 22 October 2025; Cristina Schepisi (ed), 'Il Costituzionalismo Digitale Tra Stati Uniti e Europa' *Unione Europea, Pluralismo e Libertà dei Media dell'era digitale* (Editoriale Scientifica 2025) 6–11; Bradford (n 2) 15.

¹² See: European Commission, 'The EU's Digital Services Act' (*European Commission*, 27 October 2022) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en> accessed 21 October 2025.

¹³ Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising.

¹⁴ Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act).

¹⁵ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

the DSA's perspective by addressing platform dominance, with the goal to impose boundaries on the monopolistic power held by major platforms as described at the beginning of this introduction. Finally, as platforms' functioning is largely based on data processing and algorithmic systems, the General Data Protection Regulation (GDPR)¹⁶ and the Artificial Intelligence Act (AI Act)¹⁷ also represent important points of reference for the purposes of this research.

Among these regulations,¹⁸ the DSA is the one most directly concerned with the opinion power of major internet intermediaries, as it governs how platforms organise, moderate, and amplify information, setting the legal boundaries for their gatekeeping function. The main question this research aims to answer is precisely whether the DSA and other recent regulatory initiatives at the EU level take adequately into account platforms' role in shaping public opinions and effectively succeed in design rules to counterbalance it. While the new rules have been widely commented from a variety of perspectives, a comprehensive analysis of their impact on the governance of information flows has not yet been proposed. To address this question, the work is structured in five chapters.

The first chapter (Chapter I) lays out the theoretical framework of the research, as partially recalled at the beginning of this introduction. It defines the notion of digital platforms and explains why they have become central actors in contemporary public life. Three main factors are identified in this regard: the platformisation of the web, the consolidation of digital markets, and the increasing relevance of digital interactions in global communications. Dominant platforms are therefore

¹⁶ 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).

¹⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

¹⁸ Bradford (n 10).

positioned as gatekeepers of an ever-growing share of global interactions, conferring on them a significant power. This power primarily consists in the ability to control access and to shape the conditions under which such interactions occur. While this gatekeeping function has implications for both commercial and non-commercial activities, it acquires particular significance when exercised over content of public relevance, as it translates into opinion power. This chapter argues that platforms' opinion power is primarily rooted in the non-neutrality of their information transmission services. In particular, it highlights how platforms exert various forms of filtering over third-party content, which can broadly be distinguished in moderation and prioritisation activities. Several examples are provided to illustrate the impact of such filtering activities on public opinion and democratic processes. Concentration in the means of information distribution has traditionally been counterbalanced by regulatory obligations designed to align their functioning with the public interest in an open, transparent, and plural public discourse. This raised the question of whether, and how, a similar framework should be extended to today's digital environment. Recent EU regulations on the digital sector seem to align with this perspective, seeking to bring platform governance closer to European fundamental values and giving rise to what may be described as a form of digital constitutionalism.

The second chapter (Chapter II) addresses the question of the liability of internet intermediaries for the content they transmit on behalf of users. Precisely because of their ability to choose and select the content they disseminate, traditional media are generally held responsible for it, through the so-called 'editorial responsibility'. Conversely, digital intermediaries have traditionally been exempted from liability for third-party illegal content. While requiring them to block illegal user content would inevitably increase their gatekeeping functions, it is important to note that under this traditional liability framework platforms retained full discretion over whether – and to what extent – they exercised these functions. This effectively granted them unilateral power in managing the transmission of content without the

corresponding legal accountability borne by traditional media. The changes introduced by the Digital Services Act for this liability regime have been examined throughout this chapter. Broadly speaking, the DSA marks a shift away from the traditionally binary approach to digital intermediaries' regulation, which revolved around exemption versus liability, towards a more nuanced model of platform accountability.¹⁹ While reaffirming the safe harbour principle, the DSA introduces new obligations that significantly increase platforms' accountability for the content they distribute, expanding the situations in which they are required to intervene. Indeed, the DSA establishes cases of 'mandatory' moderation at EU level, including obligations resulting from injunctions (Article 10), notice-and-action mechanisms (Article 16), and trusted flaggers (Article 22). These provisions have the merit of strengthening external control over the legality of online content, contributing to a broader diffusion of power in the digital public sphere. Furthermore, under the provisions on systemic risks, platforms designated as VLOPs or VLOSEs have a duty to assess and, where necessary, limit the possible spread of illegal content through their services, as well as to prevent other negative impacts on civic debate and electoral processes. The scope of this obligation is debated, particularly regarding the emergence of a general obligation to moderate content. However, there is an emerging consensus that these provisions do not require the removal of content but rather require platforms to take all necessary measures to avoid facilitating or amplifying its spread (e.g., adapting virality mechanisms).

The third chapter (Chapter III) addresses the regulation of moderation activities performed by digital platforms. Content moderation is a classical function of the media, traditionally exercised by editors and broadcasters to avoid the spread of harmful content. Digital platforms now perform a similar role, applying their terms and conditions to remove or restrict not only illegal content but also material

¹⁹ Martin Husovec, 'Will the DSA Work? On Money and Effort' in Joris van Hoboken (ed), *Putting the Digital Services Act Into Practice* (Verfassungbooks 2023) 21.

deemed inconsistent with their community standards. This practice constitutes a direct expression of their opinion power, as platforms can unilaterally decide which content should not be transmitted. Such a decision can become particularly impactful considering their market dominance, meaning that moderation decisions can result in the loss of access to a crucial communication channel, effectively excluding certain voices or perspectives from the public conversation. Moderation on digital platforms has long been plagued by issues of transparency, accountability, lack of redress mechanisms for users, and biased decision-making. The Digital Services Act is the first regulation to introduce a comprehensive set of obligations for platforms in this regard, thereby granting users specific rights related to content moderation. Additional protections are provided by the European Media Freedom Act, which grants enhanced safeguards to users who qualify as media entities, seeking to ensure that lawful journalistic content is not arbitrarily removed. The analysis of these instruments leads to the conclusion that spontaneous content moderation by digital platforms is fully legitimised under the new EU's regulatory framework, but also subject, for the first time, to a significant control. Such rules consist primarily in due process safeguards, such as the duty to state reasons in the case of content removal, and the obligation to provide access to redress mechanisms, alongside multiple transparency requirements. From a substantive perspective, conversely, the regulatory framework remains more limited, since it is largely silent on the unilateral rule-making power of platforms, which nonetheless represents a major source of platforms' opinion power. However, the newly introduced obligation to respect fundamental rights in content moderation, together with the systemic risks management obligations, could allow for an external scrutiny on platforms' terms and conditions. This greater emphasis on procedural

safeguards has led some scholars to describe the DSA as adopting a ‘procedure before substance’ approach.²⁰

The fourth issue analysed concerns the regulation of ranking, prioritisation and recommendations practices (Chapter IV). The way platforms prioritise and recommend content is today the primary mechanism through which they shape the information users receive. This process is largely driven by algorithmic systems designed by platforms to maximise their own profits, namely by keeping users online longer and increasing advertising revenue. These systems heavily rely on the collection and processing of personal data, using complex profiling to deliver customised feeds. These practices raise significant concerns about transparency, user autonomy, and the vulnerability of democratic processes to manipulation. A range of legal instruments has been introduced to address different dimensions of this issue. Rules on data use and profiling originate primarily from the GDPR, but further obligations are imposed by the Digital Services Act, the Digital Markets Act, and the Regulation on the Transparency and Targeting of Political Advertising. The resulting framework is complex and multi-layered. Generally speaking, the foundational principles established by the GDPR in 2016 for personal data processing have evolved along two main axes. First, additional safeguards have been introduced to ensure that user consent to data processing is genuinely free, thereby reinforcing individual autonomy. This is essentially achieved by requiring platforms to offer an equivalent service even when users refuse certain targeting practices.²¹ Second, some targeting practices have been prohibited outright, irrespective of user consent.²² This regulatory shift marks a decisive move away from a purely contractual model based on the formal freedom of the parties, aligning

²⁰ Pietro Ortolani, ‘If You Build It, They Will Come: The DSA “Procedure Before Substance” Approach’ in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023) 154.

²¹ See: Article 38 of the DSA, Article 5(2) of the DMA, Article 18 of the PAR.

²² See: Article 26 and 38 of the DSA.

instead with legal frameworks addressing structural contractual asymmetries, such as consumer protection and competition law. In addition to these restrictions, transparency obligations regarding recommender systems have been introduced.²³ However, the degree of actual control conferred upon users remains limited. While platforms are required to inform users of the possibility to influence recommendation systems, none of the existing regulations compel them to offer such functionalities in the first place. Indeed, the ‘equivalent alternative’ requirement tends to function more as a rigid binary choice than a mechanism enabling users to personalise recommendation parameters according to their preferences. In this context, it must be noted that the systemic risks management obligations applicable to VLOPs and VLOSEs can represent the tool to alter this regulatory landscape. Ultimately, as demonstrated by the *pay-or-okay* clause introduced by Meta, the practical impact of these provisions will heavily depend on their implementation by platforms and the assessment made by supervisory authorities.

The fifth and final chapter (Chapter V) addresses the enforcement structure of relevant regulations. The rules introduced by the EU’s digital framework are broad and ambitious, but their real impact depends on how they are implemented and supervised in practice. Experience with pioneering instruments such as the GDPR has shown that advanced regulatory models can suffer from under-enforcement and widespread non-compliance limiting their effectiveness. However, it must be noted that the Digital Services Act Package places a strong emphasis on enforcement. For major players enforcement powers are centralised in the hands of the European Commission, marking a significant shift from the past. However, ensuring effective oversight remains complex, as the DSA must interact with other complementary regulations without the benefit of a single horizontal enforcement framework.

²³ See: Article 26 and 27 of the DSA and Article 18 of the PAR.

Questions of coordination, overlapping competences, and the risk of regulatory fragmentation remain open.

Before delving into the analysis of regulatory provisions, it is essential to first understand the role that digital platforms play in today's public sphere and information ecosystem. Any attempt to assess the adequacy of legal interventions must be grounded in a clear understanding of the nature, functions, and influence of these actors.

I. DIGITAL PLATFORMS AS INFORMATION GATEKEEPERS: OPINION POWER IN THE DIGITAL REALM

The essential function of digital platforms is to facilitate intermediation among different users on the internet. These users may belong to the same category, such as individuals interacting on social media, or they may belong to different groups, as in the case of business entities and consumers. Qualifying platform services as intermediaries implies that they neither produce nor transmit their own content; rather, they provide a digital infrastructure that enables other parties to exchange information. While the term ‘platform’ is often employed to refer to a wide range of services with varying characteristics, for the purpose of this research the notion of platform service (or, simply, ‘platform’) will follow the definition provided by the Digital Services Act, Article 1(i). According to this definition, platform services are digital services that store information provided by a recipient, with the ability to make that information publicly available at the recipient’s request. Accordingly, platforms are understood here to possess two essential features: (1) the carriage of third-party content; (2) the potential public dissemination of that content. The focus of this research on such services stems from their ubiquity in contemporary social, economic and political life.

While the early web carried a promise of democratisation and disintermediation,²⁴ its space has been largely appropriated by powerful private actors. In theory, the internet remains ‘open’; however, in practice, for most users, internet access and

²⁴ Habermas (n 2) 46; John Perry Barlow, ‘A Declaration of the Independence of Cyberspace’ <<https://www.eff.org/cyberspace-independence>> accessed 21 October 2025; Lucas D Introna and Helen Nissenbaum, ‘Shaping the Web: Why the Politics of Search Engines Matters’ (2000) 16 *The Information Society* 169, 169 <<https://doi.org/10.1080/01972240050133634>> accessed 26 June 2025; C Edwin Baker, *Media Concentration and Democracy: Why Ownership Matters* (Cambridge University Press 2006) 100 <<https://www.cambridge.org/core/books/media-concentration-and-democracy/31C4D0D3746C15CA199EF62B9772B068>> accessed 13 November 2024; Wu, *The Master Switch* (n 5) 318.

use are intermediated from beginning to end.²⁵ The structure of what is commonly referred to as ‘Web 2.0’, in contrast to the earlier era of the ‘open web’, is characterised by a small number of dominant platforms that possess the vast majority of digital markets’ shares. As a result, most online access and interaction today occur through these platforms and, moreover, through a highly concentrated few. At the same time, as both the economy and social life become increasingly digitalised, a growing share of global communication and transactions takes place online, and more specifically, on these major platforms. This concentration grants them substantial gatekeeping power, allowing them to shape the rules of the internet and the dynamics of online interactions.

Therefore, the ubiquity of digital platforms stems from various factors, including the platformisation of the economy, the consolidation of digital markets, and the digitalisation of global interactions, as analysed in following Section 1. This structural intermediary position confers platforms a gatekeeping function, a role which is inherently associated with power. A specific dimension of this power is what can be defined as ‘opinion power’, whose meaning and concrete manifestations are analysed in Section 2.

1. A PLATFORM ECONOMY AND INTERMEDIATED ACCESS TO INFORMATION

The emergence of a ‘platform economy’ implies an increased intermediation of human interactions: exchanges are no longer direct but shaped by the functioning of platform infrastructures. While the first part of this section (1.1) examines the factors illustrating the emergence of this type of economy, the second part (1.2) introduces the concept of gatekeeping, especially regarding non-commercial information.

²⁵ Cohen (n 3) 41.

1.1. A HIGHLY CONCENTRATED DIGITAL ECONOMY: BIG TECH'S DOMINANCE IN ECONOMIC AND SOCIAL INTERACTIONS

The centrality of major platforms in today's public sphere is linked to three crucial factors: (a) platform-type services account for the majority of web traffic; (b) digital markets are highly concentrated, with a handful of platforms holding the vast majority of market shares; and (c) an ever-growing part of human interactions unfolds online. While market share is the most common indicator of dominance, other metrics such as time spent, number of active users, and advertising revenues also provide valuable insights into the scale and influence of major platforms.²⁶

Regarding the platformisation of the web [point (a)], it is noteworthy that among the twenty most visited websites worldwide in 2024, only one (Netflix) is not a platform within the meaning adopted in this research.²⁷ As for market consolidation in the digital sector [point (b)], this has long been a matter of concern, largely driven by structural characteristics of the platform economy and digital markets that foster winner-takes-all dynamics.²⁸ These characteristics include economies of scale and scope, data-driven business models, network effects, and high switching costs.²⁹ First, digital platform markets are characterised by economies of scale: the high fixed costs of developing the service are coupled with a near-zero marginal costs for providing it to an additional user, which means that the average costs fall

²⁶ John M Newman, 'Antitrust in Attention Markets: Definition, Power, Harm' (2020) Paper No. 3745839 University of Miami Legal Studies Research 28 <Available at SSRN: <https://ssrn.com/abstract=3745839> or <http://dx.doi.org/10.2139/ssrn.3745839>>.

²⁷ Thiago Bianchi, 'Global Top Websites by Monthly Visits 2024' <<https://www.statista.com/statistics/1201880/most-visited-websites-worldwide/>> accessed 24 June 2025.

²⁸ Jason Furman, *Unlocking Digital Competition* (2019) 35 <<https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel>> accessed 24 June 2025; Patrick Barwise and Leo Watkins, 'The Evolution of Digital Dominance. How and Why We Got to GAFA' in Damian Tambini and Martin Moore, *Digital Dominance. The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018) 22.

²⁹ Pietro Manzini, 'Il Digital Market Act Decodificato' *Unione europea 2020 - I dodici mesi che hanno segnato l'integrazione europea* (Cedam Kluwer 2021).

dramatically as the user base expands.³⁰ Similar consolidation trends have historically characterised communication and media markets, where fixed costs are considerably significant compared to marginal costs.³¹ In addition to this, economies of scale in the platform economy are closely tied to the collection and use of user data, the monetisation of which in the advertising market constitutes the business model of these platforms.³² In this context, large datasets represent an advantage for the incumbent, enabling the improvement of the service provided, also by making it more targeted for users ('feedback loop').³³ Another key feature of digital platform markets that drives them toward consolidation is the 'network effect': as connection itself is the service provided to users, the value of the service increases as the number of users grows. Finally, both inherent and induced high switching costs, often coupled with lock-in effects, include users' reliance on familiar systems, the loss of personalisation when switching services, as well as incompatibility and limited data portability across platforms.³⁴

Such a tendency toward consolidation is reflected in the distribution of market shares. In 2023, Amazon, for example, held 37.6% of the e-commerce market share in the United States, with Walmart, the second-largest competitor, at just 6.5%.³⁵ In 2024, Google commanded 90% of the European search engines market, and 85% in the United States.³⁶ In the social media sector, Meta-owned platforms (Facebook and Instagram) account for 80.46% of market share worldwide, followed by Twitter

³⁰ Furman (n 28) 32.

³¹ Baker (n 24).

³² Shoshana Zuboff, *Il capitalismo della sorveglianza* (2023rd edn, Luiss University Press 2019). See also *infra*: Chapter IV.

³³ Furman (n 28) 33.

³⁴ For a history on how major platforms acquired their dominance, see: Barwise and Watkins (n 28) 29.

³⁵ Statista Research Department, 'Largest Online Retailers in the U.S. 2023' <<https://www.statista.com/statistics/274255/market-share-of-the-leading-retailers-in-us-e-commerce/>> accessed 24 June 2025.

³⁶ Thiago Bianchi, 'Online Search Market in Europe – Statistics & Facts' (*Statista*, 27 May 2024) <<https://www.statista.com/topics/11065/online-search-market-in-europe/>> accessed 7 January 2025.

and Pinterest at around 7%, YouTube at 4% and Reddit at 1%.³⁷ Such data have led scholars to variously define these companies as near-monopolists³⁸ or moligopolists.³⁹ The consolidation of digital markets has also been reinforced by deliberate corporate strategies,⁴⁰ such as a significant merger and acquisition activity,⁴¹ whereby dominant platforms have systematically absorbed potential competitors – as illustrated by some paramount cases, such as Meta’s acquisitions of Instagram and WhatsApp,⁴² or Google’s acquisitions of YouTube.⁴³ These dynamics have also prompted several antitrust proceedings against major platforms, both in the United States and in the European Union.⁴⁴

³⁷ StatCounter, ‘Social Media Stats Worldwide’ <<https://gs.statcounter.com/social-media-stats/all/worldwide/2022>> accessed 24 June 2025.

³⁸ Justus Haucap and Ulrich Heimeshoff, ‘Google, Facebook, Amazon, eBay: Is the Internet Driving Competition or Market Monopolization?’ (2014) 11 *International Economics and Economic Policy* 2. Martin Moore, *Tech Giants and Civic Power* (CMCP, Policy Institute, King’s College London, 2016), 13, <https://doi.org/10.18742/pub01-027>. Martin Moore, *Tech Giants and Civic Power* (CMCP, Policy Institute, King’s College London 2016) 13. Moore (n 7) 13.

³⁹ Nicolas Petit, *Big Tech and the Digital Economy: The Moligopoly Scenario* (Oxford University Press 2020).

⁴⁰ Barwise and Watkins (n 28) 30.

⁴¹ Furman (n 28) 24–31.

⁴² Sarah Hinck, ‘Big Tech Antitrust Scrutiny Across the Atlantic’ [2025] *Verfassungsblog* <<https://verfassungsblog.de/big-tech-antitrust-scrutiny-across-the-atlantic-meta-ftc-tech/>> accessed 22 October 2025.

⁴³ Tim Wu and Stuart A Thompson, ‘The Roots of Big Tech Run Disturbingly Deep’ *The New York Times* (7 June 2019) <<https://www.nytimes.com/interactive/2019/06/07/opinion/google-facebook-mergers-acquisitions-antitrust.html>, <https://www.nytimes.com/interactive/2019/06/07/opinion/google-facebook-mergers-acquisitions-antitrust.html>> accessed 24 June 2025.

⁴⁴ For instance, recently, the Justice Department’s Antitrust Division of the United States has scrutinised the legitimacy of Google’s exclusive contracts for the distribution of some of its services (United States Department of Justice, ‘Department of Justice Wins Significant Remedies Against Google’ <<https://www.justice.gov/opa/pr/departments-justice-wins-significant-remedies-against-google>> accessed 15 September 2025.). Within the EU, several antitrust proceedings have been opened against major internet intermediaries, for instance: European Commission, ‘Antitrust: Commission Accepts Commitments by Amazon’ (*European Commission*, 20 December 2022) <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777> accessed 22 October 2025; European Commission, ‘Commission Fines Google €2.95 Billion over Abusive Practices in Online Advertising Technology’ (*European Commission*, 5 September 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1992> accessed 22 October 2025; European Commission, ‘Commission fines Meta’ (*European Commission*, 14 November 2024) <https://ec.europa.eu/commission/presscorner/detail/sl/ip_24_5801> accessed 22 October 2025.

With respect to the growing relevance of the digital economy [point (c)], it is notable that the world's six largest corporations by market capitalization all belong to the tech sector.⁴⁵ While top position has been recently taken by Nvidia, a company producing essential hardware for developing AI systems,⁴⁶ the other five positions have been consistently held over the past decade by Google (Alphabet), Apple, Facebook (Meta), Amazon and Microsoft. Together, these companies are commonly referred to by the acronym 'GAFAM', or more broadly as 'Big Tech' or 'Tech Giants',⁴⁷ terms that have come to symbolise the concentration of economic power in the hands of a few dominant corporations within to the digital sector.

There are several other data points that can illustrate the growing relevance of online interactions and digital platforms in public life. First, the number of internet users and social media users steadily grows worldwide.⁴⁸ Second, looking at the advertisement revenue, a key indicator for the communication industry dynamics,⁴⁹ recent data show that Google, Meta, and Amazon together generated over 60% of global digital advertising revenue in 2023, capturing nearly \$417 billion in ad spend.⁵⁰ More broadly, digital ads are estimated to have accounted for 72.7% of worldwide ad investment in 2024.⁵¹ Another point worth noting, and particularly

⁴⁵ CompaniesMarketCap, 'Companies Ranked by Market Cap' (*CompaniesMarketCap.com*) <<https://companiesmarketcap.com/>> accessed 15 September 2025.

⁴⁶ Kif Leswing and Samantha Subin, 'Nvidia Briefly Touched \$4 Trillion Market Cap for First Time' (*CNBC*, 9 July 2025) <<https://www.cnbc.com/2025/07/09/nvidia-4-trillion.html>> accessed 15 September 2025. Some reflections on the role of AI systems will also be provided throughout the analysis.

⁴⁷ Moore (n 7); Petit (n 39).

⁴⁸ As of February 2025, 5.56 billion individuals worldwide were internet users, which amounted to 67.9% of the global population, while 5.24 billion, or 63.9% of the world's population, were social media users (Ani Petrosyan, 'Internet and Social Media Users in the World 2025' (*Statista*) <<https://www.statista.com/statistics/617136/digital-population-worldwide/>> accessed 30 July 2025.)

⁴⁹ On the multi-sided nature of the markets where platforms operate, see also *infra*: Section 2.1.

⁵⁰ Jastra Kranjec, 'Google, Meta, and Amazon Generate Over 60% of Global Digital Advertising Revenue' (*Stocklytics*, 29 February 2024) <<https://stocklytics.com/content/google-meta-and-amazon-generate-over-60-of-global-digital-advertising-revenue/>> accessed 24 June 2025.

⁵¹ Simon Kemp, 'Digital 2025: Global Advertising Trends' (*DataReportal – Global Digital Insights*, 5 February 2025) <<https://datareportal.com/reports/digital-2025-sub-section-global-advertising-trends>> accessed 24 June 2025.

relevant for the object of this research, concern news sources: in 2025, according to the annual *Digital News Report* published by the Oxford's Reuters Institute for the Study of Journalism, social media has become the most common source of news consumption in the United States, overtaking television for the first time.⁵² In the EU, in 2023, television remained the most common media channel across most Member States, but social media platforms account for a growing share, especially among young people.⁵³

These are merely some of the many indicators of the growing importance of the digital economy, as well as of the increasing relevance of communication on social media relative to legacy media. The central role of digital platforms in channelling a significant share of global interactions places them in a structural position of intermediation, which inherently entails the capacity to control access, *i.e.* to act as gatekeepers, a notion further explored in the following section.

1.2. GATEKEEPING POLITICALLY RELEVANT INFORMATION: OPINION POWER OF SOCIAL MEDIA PLATFORMS AND SEARCH ENGINES

As seen in the previous section, platforms are essential intermediaries in contemporary social and economic interactions. Intermediation is hardly neutral: control over such critical infrastructures is inherently associated with power, since it comes with the ability to determine the rules governing access and to 'shut the gate' when deemed necessary. Moreover, platforms not only control access to their infrastructure, but also, crucially, set the rules for its functioning.⁵⁴

⁵² Nic Newman, 'Digital News Report 2025' (Reuters Institute for the Study of Journalism 2025) 11 <<https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025>> accessed 24 June 2025.

⁵³ Eurobarometer, 'Media & News Survey 2023' (European Parliament 2023) Flash Survey <<https://europa.eu/eurobarometer/surveys/detail/3153>>. For more recent data, it is possible to look at national-specific reports, such as, for Italy: Giacomo Lasorella, 'Relazione annuale 2025 sull'attività svolta e sui programmi di lavoro' VII <https://www.agcom.it/sites/default/files/documenti/relazione_annuale/RELAZIONE%20ANNUALE%202025_0.pdf>.

⁵⁴ Helberger, Kleinen-von Königslöw and Noll (n 4) 57.

This gatekeeping power becomes particularly significant in light of the dominant market position held by these platforms, which renders their infrastructures effectively ‘critical’. In highly competitive markets, a multiplicity of actors would be able to set operational rules, and users could select the most favourable ones; denial of access to a single platform would therefore not entail major consequences for market participation. Conversely, market dominance magnifies the impact of gatekeepers’ choices, positioning them primary governors of the digital environment. In this context, the private rules established by large corporations such as Apple, Facebook and Google have assumed the role of global standards, unilaterally shaping markets, information flows and social interactions.⁵⁵

Since gatekeeping power is intrinsically linked to critical infrastructures, namely those constituting the only channels through which markets can be effectively accessed, this research focuses on Big Tech providing platform services. The definition of ‘Big Tech’ is not always clear-cut; however, recent EU regulations have begun to provide a legal qualification for these actors, acknowledging the need for a specific regulatory framework. Such qualification emerges in both the Digital Services Act, through the categories of ‘Very Large Online Platforms’ and ‘Very Large Search Engines’,⁵⁶ and in the Digital Markets Act, which introduces the notion of ‘gatekeepers’.⁵⁷ While these two definitions do not entirely overlap, they both constitute valid point of reference for addressing issues related to platforms’ control over information flows. However, since market access does not constitute the primary concern of this research, the definition adopted by the DSA, which is based solely on the number of average monthly users, is better suited for the purposes of this analysis.

⁵⁵ Cohen (n 3) 45.

⁵⁶ See *infra*: Chapter II, Section 2.1.

⁵⁷ See *infra*: Chapter IV, Section 2.1.

Indeed, gatekeeping power extends beyond the commercial sphere, significantly affecting not only businesses and consumers, but also the circulation of non-commercial information. This research primarily focuses on platforms' control over non-commercial, or not exclusively commercial, information flows and content, such as those characterising the media ecosystem. This category of information can be broadly referred to as 'political', in the classical sense of the term, namely information that sustains public life and holds relevance for the community and the governance of society.⁵⁸

From this perspective, social media platforms and search engines are particularly relevant.⁵⁹ This does not mean, however, that marketplaces such as Amazon or app stores like the Apple Store lack influence over content transmission. Certain examples illustrate this point: for instance, Facebook's app must comply with Apple's App Store terms and conditions to operate on iOS devices, including restrictions on nudity.⁶⁰ Similarly, Amazon's selection and ranking of books and e-books significantly shape the circulation of cultural content.⁶¹ Nonetheless, their influence on content transmission appears less systematic and pervasive than that exerted by social media platforms and search engines.⁶² The prominent role of social media platforms and search engines in content transmission is connected to their intermediary function between content providers and users,⁶³ including with regard to access to news and political information. For this reason, scholars have

⁵⁸ Aristotele, *Politica* (1993rd edn, Economica Laterza 4th century BCE).

⁵⁹ This includes video-sharing platforms, such as YouTube, which are generally considered as a mixture between social media and search engines.

⁶⁰ Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (2018) 188.

⁶¹ Gillespie (n 60) 188.

⁶² In any case, many of the conclusions drawn in this work may equally apply to these other platforms.

⁶³ However, it is important to note that, since platforms operate as one-to-one medium (Manuel Castells, 'Communication, Power and Counter-Power in the Network Society' (2007) 1 *International Journal of Communication* 29 <<https://ijoc.org/index.php/ijoc/article/view/46>> accessed 13 November 2024.) the categories of content providers and content recipients are often interchangeable.

proposed the term ‘information intermediaries’ to specifically describe these actors.⁶⁴

The intermediation power of search engines is particularly relevant, since almost all access to online content is facilitated through them. While users may not engage with social media platforms during every online session, they almost invariably rely on a search engine to locate and access websites and information across the web. Moreover, as previously noted, the search engine’s market is even more concentrated than the social media sector, with Google holding approximately 90% of market shares in Europe and 85% in the United States.⁶⁵ This is the reason why the selection of content made by Google is particularly relevant for the global circulation of information. In this perspective, Jeffrey Rosen in 2012 referred to ‘the Deciders’:⁶⁶

‘Until recently, the person who had more power to determine who may speak and who may be heard around the world was not a president or king or Supreme Court Justice. She was Nicole Wong, who was deputy general counsel at Google until her recent resignation. Her colleagues called her “the Decider.” Nicole Wong was the Decider, who was awoken in the middle of the night to decide what content goes up or comes down, not only on Google.com, not only on each of the national Googles that are operated around the world, such as Google.fr, Google.de, but also what goes up or comes down on YouTube, which Google bought in 2006.’

Similarly, the prominent antitrust and media law scholar Tim Wu had stated that Google is ‘*the current custodian of the Master Switch*’.⁶⁷ However, Tim Wu’s book also warned against the constantly evolving nature of dominance in the communication industry, largely shaped by disruptive technological innovations.⁶⁸ In this perspective, the emerging role of generative AI systems deserves particular

⁶⁴ Helberger, Kleinen-von Königslöw and Noll (n 4); Moore (n 7) 9.

⁶⁵ Bianchi (n 36).

⁶⁶ Jeffrey Rosen, ‘The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google’ (2012) 80 Fordham Law Review 1525, 1536 <<https://ir.lawnet.fordham.edu/flr/vol80/iss4/1>>.

⁶⁷ Wu, *The Master Switch* (n 5) 282.

⁶⁸ Wu, *The Master Switch* (n 5) 6.

attention. The launch of ChatGPT may have already marked a turning point in the global structure of content transmission and accessibility, as models like ChatGPT are increasingly used as substitutes for search engines,⁶⁹ while traditional search engines such as Google begun integrating AI-generated summaries as the firsts result displayed to users' queries.⁷⁰ Unlike digital platforms, these technologies can display third-party links, but can also generate their own outputs based on the processing of such external content. In this case, they perform a selective elaboration of information, positioning themselves at the intersection of content production, intermediation and distribution. For now, however, generative AI's reach in the news environment appears limited: in 2025, only 4% of respondents reported using ChatGPT (the most popular tool) to access news, and just 2% reported using Google Gemini.⁷¹ These figures contrast with complaints by news providers claiming that AI-generated summaries on Google have significantly reduced traffic on their websites, as users increasingly rely on the answer displayed by Google.⁷² Moreover, OpenAI has recently launched Sora, a generative-AI-based social media platform where visual content is created artificially rather than by

⁶⁹ ChatGPT has recently launched its own browser, ChatGPT Atlas: Lisa Eadicicco, 'The Battle for the Future of the Internet Is Underway | CNN Business' (CNN, 22 October 2025) <<https://www.cnn.com/2025/10/22/tech/openai-chatgpt-atlas-browser-google-chrome-ai>> accessed 27 October 2025.

⁷⁰ The Economist, 'AI Is Killing the Web. Can Anything Save It?' *The Economist* (14 July 2025) <<https://www.economist.com/business/2025/07/14/ai-is-killing-the-web-can-anything-save-it>> accessed 15 September 2025; Anna Lieb and Athena Chapekis, 'Google Users Are Less Likely to Click on Links When an AI Summary Appears in the Results' (Pew Research Center, 22 July 2025) <<https://www.pewresearch.org/short-reads/2025/07/22/google-users-are-less-likely-to-click-on-links-when-an-ai-summary-appears-in-the-results/>> accessed 11 September 2025. The fact that Google has integrated its own AI overview system and places its summaries on the top of the result page can pose significant antitrust concerns.

⁷¹ Newman (n 52) 30.

⁷² Foo Yun Chee, 'Exclusive: Google's AI Overviews Hit by EU Antitrust Complaint from Independent Publishers' *Reuters* (4 July 2025) <<https://www.reuters.com/legal/litigation/googles-ai-overviews-hit-by-eu-antitrust-complaint-independent-publishers-2025-07-04/>> accessed 11 September 2025; Bobby Allyn, 'Online News Publishers Face "extinction-Level Event" from Google's AI-Powered Search' *NPR* (31 July 2025) <<https://www.npr.org/2025/07/31/nx-s1-5484118/google-ai-overview-online-publishers>> accessed 11 October 2025. A similar complaint has been made by Wikipedia: Marshall Miller, 'New User Trends on Wikipedia' (*Diff*, 17 October 2025) <<https://diff.wikimedia.org/2025/10/17/new-user-trends-on-wikipedia/>> accessed 22 October 2025.

human users,⁷³ and have recently declared it will start display advertised content on ChatGPT.⁷⁴ Indeed, such systems have already demonstrated potential harms and arbitrariness in their content selection,⁷⁵ as well as the possibility to use their bottleneck function to influence public opinion.⁷⁶ In this context, the European Commission appears to be aware of the need to extend certain rules governing content curation practices to generative AI systems, but can currently do so only insofar as they also qualify as digital platforms.⁷⁷ A first investigation of this kind has been opened in relation to Grok, a generative AI system integrated into the platform X, following serious concerns regarding the generation of illegal content.⁷⁸ In light of these developments, this research offers some reflections on the possible extension of the regulatory framework governing digital platforms to generative AI systems, as part of the broader discussion on the gatekeeping power of digital services.

⁷³ Lisa Eadicicco, 'The next Era of Social Media Is Coming. And It's Messy so Far' *CNN* (11 October 2025) <<https://www.cnn.com/2025/10/11/tech/openai-sora-2-meta-ai-slop-social-media>> accessed 21 October 2025.

⁷⁴ OpenAI, 'Test degli annunci in ChatGPT' (*Open AI*, 9 February 2026) <<https://openai.com/it-IT/index/testing-ads-in-chatgpt/>> accessed 13 February 2026.

⁷⁵ Sam Altman [@sama], 'We Made ChatGPT Pretty Restrictive to Make Sure We Were Being Careful with Mental Health Issues. We Realize This Made It Less Useful/Enjoyable to Many Users Who Had No Mental Health Problems, but given the Seriousness of the Issue We Wanted to Get This Right. Now That We Have' <<https://x.com/sama/status/1978129344598827128>> accessed 21 October 2025; Robert Booth and Robert Booth UK technology editor, 'ChatGPT "Upgrade" Giving More Harmful Answers than Previously, Tests Find' *The Guardian* (14 October 2025) <<https://www.theguardian.com/technology/2025/oct/14/chatgpt-upgrade-giving-more-harmful-answers-than-previously-tests-find>> accessed 21 October 2025.

⁷⁶ Newton Casey, 'The Campaign to Make It Illegal for ChatGPT to Criticize Trump' (*Platformer*, 15 July 2025) <<https://www.platformer.news/andrew-bailey-chatgpt-trump-jawboning-legal-case/>> accessed 15 September 2025; *Il Post*, 'Elon Musk continua a bisticciare col suo chatbot' *Il Post* (1 July 2025) <<https://www.ilpost.it/2025/07/01/grok-elon-musk/>> accessed 11 September 2025.

⁷⁷ Euractiv, 'Commission Checking If ChatGPT Falls under EU Online Governance Rules' (*Euractiv*, 22 October 2025) <<https://www.euractiv.com/news/commission-checking-if-chatgpt-falls-under-eu-online-governance-rules/>> accessed 27 October 2025.

⁷⁸ European Commission, 'Commission Investigates Grok and X's Recommender Systems under the Digital Services Act' <https://ec.europa.eu/commission/presscorner/detail/en/ip_26_203> accessed 3 February 2026.

With regard to the role of certain platforms as information intermediaries for politically relevant content, several examples illustrate how crucial they have become in this domain. Today, all public or private actors operate through these platforms, as failure to do so risks a loss of relevance and recognition; and this includes most of government agencies, which maintain an active presence on social media.⁷⁹ Then, the privileged position of digital platforms as intermediaries of public communication becomes particularly evident in times of crisis. During natural disasters, such as earthquakes, or the Covid-19 pandemic, public authorities have often relied on them as mass communication tools to mitigate the negative effects of crises and to disseminate reliable information.⁸⁰ A further example of their central role can be found in recent armed conflicts, where all parties involved have sought the broadest possible dissemination of their narratives through online platforms, which have become key arenas for propaganda and information warfare.⁸¹ Perhaps the most prominent example of platforms' function, however, concerns their use in political campaigns.⁸² In this light, it is worth recalling Mark Zuckerberg's 2017 Letter on Facebook's Global Ambitions, which explicitly acknowledges the platform's influence over electoral processes worldwide:

'In recent campaigns around the world – from India and Indonesia across Europe to the United States – we've seen the candidate with the largest and most engaged following on Facebook usually wins. Just as TV became the primary medium for

⁷⁹ The trend is increasingly consolidating since 2011 (Moore (n 7) 10.), with a major acceleration after Covid-19 pandemic.

⁸⁰ More specific examples can be found in: Natali Helberger, 'The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power' (2020) 8 Digital Journalism 842, 848 <<https://doi.org/10.1080/21670811.2020.1773888>> accessed 13 November 2024; Moore (n 7) 27; Mike Ananny, 'From Noxious to Public? Tracing Ethical Dynamics of Social Media Platform Conversions' (2015) 1 Social Media + Society <<https://doi.org/10.1177/2056305115578140>> accessed 13 November 2024.

⁸¹ See *infra*: Chapter III.

⁸² Moore (n 7) 36.

civic communication in the 1960s, social media is becoming this in the 21st century'.⁸³

Conceptualising certain platforms as information intermediaries transmitting politically relevant content naturally raises the question of the extent to which their position may be analogous to that of traditional media. As their very name suggests, media perform an intermediary function between governing institutions and the electorate to whom institutions are accountable. In democratic societies, the media constitute the essential infrastructure of the public sphere,⁸⁴ namely the space in which citizens are exposed to competing political viewpoints and are thereby enabled to exercise their decision-making power in an informed manner, primarily through voting.⁸⁵ This space lies at the core of deliberative democracy, where political legitimacy is grounded in the discursive and agonistic character of public opinion formation.⁸⁶ The role of the media lies in the production and circulation of such competing viewpoints, as well as in the organisation of collective attention around certain issues, referred to as '*agenda-setting*' capacity.⁸⁷ Consequently, while the media do not directly exercise decision-making authority, they are closely connected to the creation and distribution of political power,⁸⁸ and have therefore been referred to as the 'Fourth Estate',⁸⁹ owing to their ability to mould the perceptions and preferences of large groups. This capacity to influence the formation of opinion among broad audiences, through the selection of the information to which they are exposed, has traditionally been characterised as '*opinion power*'.⁹⁰ Naturally, the larger the audience a single media actor can

⁸³ Mark Zuckerberg, 'Building Global Community' (*Facebook*, 5 May 2021) <<https://www.facebook.com/notes/3707971095882612/>> accessed 4 March 2025. Cited in: Helberger (n 80) 849.

⁸⁴ Baker (n 24) 6.

⁸⁵ Habermas (n 2) 20.

⁸⁶ Habermas (n 2) 20, 23, 38.

⁸⁷ Habermas (n 2) 26.

⁸⁸ Castells (n 63) 5.

⁸⁹ A quote famously attributed to Edmund Burke by Thomas Carlyle, *On Heroes, Hero-Wo and the Heroic in History* (1906th edn, Longmans 1841) 158.

⁹⁰ Helberger (n 80) 846.

influence, the greater its power. For this reason, the notion of opinion power is intrinsically linked to the principle of pluralism, which requires a balanced distribution of the influence over public opinion.⁹¹

Against this background, the role of digital platforms as intermediaries of public communication brings them conceptually close to the media sector. As discussed in the following paragraph, their gatekeeper position is likewise connected to the exercise of opinion power,⁹² albeit with specific characteristics. The significance of these actors is therefore not confined to their economic role but extends to their broader impact on societies and the functioning of democracies, an influence that has also been described as ‘civic power’.⁹³

2. PLATFORMS’ OPINION POWER AND THE PUBLIC INTEREST

According to the definition of platforms provided in the introduction of this chapter, namely as digital services enabling the storage and public transmission of third-party information, their opinion power must be framed primarily in terms of content distribution rather than content production. Indeed, the opinion power associated with the media lies not only in their capacity to produce content, but also in their control over its distribution. Media distributors shape the informational environment by determining which content circulates within a given society and by deciding the priority accorded to different pieces of information. In this sense, distributors exercise an agenda-setting power at least equal to that of content producers, as their control over access to distribution channels enables them to function as gatekeepers of public information.⁹⁴

The first part of this section (2.1) examines how digital platforms exercise this gatekeeping power, focusing on the filtering mechanisms through which they select

⁹¹ Helberger (n 80) 846; Baker (n 24).

⁹² Helberger and others (n 6).

⁹³ Moore (n 7) 22.

⁹⁴ Moore (n 7) 29.

and prioritise third-party content, with a potential impact on public opinion. The second part (2.2) then shows how the role of information distributors has traditionally attracted regulatory attention and analyses how the European Union has decided to intervene to this regard.

2.1. MODERATION AND PRIORITISATION: CONTENT CURATION PRACTICES BY THE GATEKEEPER

Despite their role in the circulation of information, platforms are not generally content producers, but rather channels for information generated by others. This does not mean, however, that platforms never exercise their opinion power in a content-producing capacity.⁹⁵ Indeed, they occasionally assume a speaker role, particularly when their direct economic interests are at stake, as in Google's campaign against proposed copyright reforms.⁹⁶ At times, this 'speaker' role has also reflected a form of civic commitment: a notable example in this regard has been Google's advocacy in support of same-sex marriage.⁹⁷ One may, of course, question the economic rationale underlying such forms of civic engagement, as they often align with platforms' reputational interests and tend to be swiftly abandoned once they become politically or socially less advantageous, as illustrated by the suppression of many corporate diversity and inclusion programmes following Donald Trump's re-election.⁹⁸ In any event, while this direct speaker capacity raises significant concerns from the perspective of opinion power, this research primarily focuses on distribution, as it remains the core function and business model of platform services.

⁹⁵ This does not mean that they do not ever produce content (see: Moore (n 7) 30.).

⁹⁶ Helberger (n 80) 846. The same author also recalls how Uber and Airbnb mobilised their users to oppose political initiatives aimed at regulating these platforms.

⁹⁷ Helberger (n 80) 846.

⁹⁸ Conor Murray, 'All The Major Companies And Orgs Dumping Their DEI Programs (Full List)' (*Forbes*) <<https://www.forbes.com/sites/conormurray/2025/04/11/ibm-reportedly-walks-back-diversity-policies-citing-inherent-tensions-here-are-all-the-companies-rolling-back-dei-programs/>> accessed 18 September 2025.

One distinctive feature of the platform environment lies in its one-to-one communicative structure,⁹⁹ whereby anyone can simultaneously act as speaker and audience, marking a true revolution in the traditional functioning of public communication.¹⁰⁰ From this perspective, platforms are empowering tools for the general public, allowing broader access to content-producing capacity and facilitating collective action. Digital intermediaries have been said, for instance, to have facilitated grassroots movements that might not have otherwise emerged, such as the Arab Springs, Black Lives Matter, or Occupy Wall Street.¹⁰¹ Yet this feature does not fundamentally alter the nature of their gatekeeping power. As Martin Moore noted, while an individual may launch a public campaign on Facebook, accessible to any of Facebook's 1.5 billion active users, it is ultimately Facebook which that retains the power enable or disable the campaign, to obscure it, or to promote it to a part or a whole of its global user base.¹⁰² Moreover, over time, the diffusion of dynamics of virality has tended to concentrate attention on a limited number of actors, referred to as influencers, thereby reintroducing communicative patterns that resemble a one-to-many model.¹⁰³ This evolution is also reflected in the growing use of the term 'social media' rather than 'social network', suggesting the declining importance of their function as horizontal means of communications.¹⁰⁴

On the other side, the dominance of platforms in content distribution also affects traditional opinion actors, such as the press and political parties. Due to media

⁹⁹ Castells (n 63).

¹⁰⁰ Habermas (n 2).

¹⁰¹ Cohen (n 3) 86.

¹⁰² Moore (n 7) 23.

¹⁰³ See also *infra*: Chapter IV. Ian Bogost, 'The Age of Social Media Is Ending' (*The Atlantic*, 10 November 2022) <<https://www.theatlantic.com/technology/archive/2022/11/twitter-facebook-social-media-decline/672074/>> accessed 21 October 2025.

¹⁰⁴ José Dijck (van), 'Social Media and the Culture of Connectivity' (*OUPblog*, 25 February 2013) <<https://blog.oup.com/2013/02/social-media-culture-connectivity/>> accessed 13 February 2026.

convergence,¹⁰⁵ news organisations have lost control over the main conduits through which their content reach audiences,¹⁰⁶ and the same holds for political actors, who now rely on platforms to communicate with the public. This dependency of traditional opinion actors on platform infrastructure has been conceptualised by Natali Helberger as a form of ‘*systemic opinion power*’.¹⁰⁷

Distributors’ influence on public opinion derives from their capacity to filter, prioritise, and organise information produced by others, shaping which content reaches users and under what conditions. Digital platforms do not make an exception in the intermediaries’ category and largely engage in their gatekeeping role. Scholars have consistently argued that content organisation, far from being an ancillary activity, is the essential service platforms provide to users.¹⁰⁸ Search engines represent the most prominent example of this, as website ranking is their core function.¹⁰⁹ Moderation and content curation practices are inherent to the digital platforms’ model and can be considered as one of their defining elements, in contrast with the chaotic navigating experience on the early web.¹¹⁰ Indeed, their success relies in offering content which is organised¹¹¹ and moderated, presenting themselves as reliable actors, as a brand,¹¹² both before individual and business clients.

The gatekeeping activities of digital platforms are exercised through two main mechanisms. The first, which applies to all information transmitted through the

¹⁰⁵ Henry Jenkins, *Convergence Culture: Where Old and New Media Collide* (NYU Press 2006) <<https://www.jstor.org/stable/j.ctt9qffwr>> accessed 18 September 2025.

¹⁰⁶ Moore (n 7) 32; Emily Bell, ‘Silicon Valley and Journalism: Make up or Break up? | Reuters Institute for the Study of Journalism’ <<https://reutersinstitute.politics.ox.ac.uk/news/silicon-valley-and-journalism-make-or-break>> accessed 21 October 2025.

¹⁰⁷ Helberger (n 80) 846.

¹⁰⁸ Gillespie (n 60) 13.

¹⁰⁹ Introna and Nissenbaum (n 24).

¹¹⁰ Napoli (n 7) 24.

¹¹¹ Napoli (n 7) 21.

¹¹² This is why Apple Store in 2010 removed not only applications containing porn, but also not well-designed ones (Gillespie (n 60) 79.).

platforms, is content organisation. On platforms, not a single piece of information escapes some form of sorting, whether based on popularity, individual user preferences or paid advertising.¹¹³ The second one, supposedly exceptional, as it concerns content deemed illegal or inconsistent with a platform's terms of use, is moderation. While moderation can be compared to a traditional form of censorship (the platform decides who can speak), content organisation is more subtle (the platform decides who gets heard).¹¹⁴ Both practices have a profound impact on freedom of expression, information pluralism, and democratic debate. Crucially, they are both tools for controlling the circulation of information, thereby influencing the formation of public opinion and, in turn, the distribution of political power. Several examples can illustrate this impact.

The paradigmatic example showing the importance of online moderation practices for public debate is probably the 'Trump ban' on Twitter.¹¹⁵ As it is well known, following the attack on Capitol Hill carried out by some of his supporters in January 2021, Donald Trump's Twitter account was suspended for inciting the commission of violent acts. The fact that a private company had been able to deprive the former president of the United States, who was also a likely candidate in the subsequent elections,¹¹⁶ of such a crucial channel of communication raised several concerns, including among EU politicians who did not sympathise with the former president's views.¹¹⁷ Furthermore, subsequent events confirmed the concerns expressed at the

¹¹³ These aspects will be examined in detail in the next chapter.

¹¹⁴ Tim Wu, 'Is the First Amendment Obsolete?' (2018) 117 Michigan Law Review 547, 554 <<https://repository.law.umich.edu/mlr/vol117/iss3/4>>.

¹¹⁵ Kevin Roose, 'In Pulling Trump's Megaphone, Twitter Shows Where Power Now Lies' *The New York Times* (9 January 2021) <<https://www.nytimes.com/2021/01/09/technology/trump-twitter-ban.html>> accessed 24 March 2025.

¹¹⁶ The presidential elections of 2024, which he won.

¹¹⁷ Euronews and AP, 'Donald Trump's Twitter Ban Is "problematic," Says Angela Merkel' (*Euronews*, 12 January 2021) <<https://www.euronews.com/my-europe/2021/01/12/donald-trump-s-twitter-ban-is-problematic-says-angela-merkel>> accessed 24 March 2025. See also: European Commission, 'Speech by the President on inauguration of new US President' (*European Commission*, 20 January 2021) <https://ec.europa.eu/commission/presscorner/detail/en/speech_21_167> accessed 25 March 2025.:

time. Indeed, the change of ownership that Twitter underwent in 2022, when it was acquired by Elon Musk,¹¹⁸ resulted in a disruptive shift in moderation policies,¹¹⁹ emphasising their arbitrariness. In this context, most of the suppressed profiles were reinstated, included Donald Trump's, allegedly to maximize freedom of expression.¹²⁰

The recent escalation of the Israeli-Palestinian conflict, following the Hamas attack on 7 October 2023, once again highlighted the risks of arbitrary moderation by digital platforms due to specific political positions of their owners. On Meta-owned platforms, content regarding Palestine has been systematically suppressed and demoted,¹²¹ employing a distorted definition of hate against Israelis, leading to restrictions on any content regarding Palestine, including human rights abuses, as reported by Human Rights Watch.¹²²

On the other side, content prioritisation and recommendation also possess a significant influence on the circulation of information. These mechanisms do not impact on the availability of information, but the likelihood that users are exposed

No matter how right it may have been for Twitter to switch off Donald Trump's account five minutes after midnight, such serious interference with freedom of expression should be based on laws and not on company rules. It should be based on decisions of parliaments and politicians and not of Silicon Valley managers.

¹¹⁸ The entrepreneur Elon Musk acquired the platform on the 27 October 2022: Kate Conger and Lauren Hirsch, 'Elon Musk Completes \$44 Billion Deal to Own Twitter' *The New York Times* (28 October 2022) <<https://www.nytimes.com/2022/10/27/technology/elon-musk-twitter-deal-complete.html>> accessed 25 March 2025.

¹¹⁹ Rebecca Kern, 'Musk Changes Twitter Suspension Policy' *Politico* (24 November 2022) <<https://www.politico.com/news/2022/11/24/musk-twitter-suspension-policy-00070819>> accessed 25 March 2025; Rebecca Kern, 'Twitter Stops Enforcing Covid-19 Misinformation Policy -' *Politico* (29 November 2022) <<https://www.politico.com/news/2022/11/29/twitter-stops-enforcing-covid-19-misinformation-policy-00071110>> accessed 25 March 2025. As further elaborated below, in the same period Twitter also exited the Code of Practice on Disinformation.

¹²⁰ Elon Musk has described himself on X (Twitter) as a 'free-speech absolutist': Elon Musk [@elonmusk], 'Starlink Has Been Told by Some Governments (Not Ukraine) to Block Russian News Sources. We Will Not Do so Unless at Gunpoint. Sorry to Be a Free Speech Absolutist.' <<https://x.com/elonmusk/status/1499976967105433600>> accessed 22 October 2025.

¹²¹ Demotion in algorithmic systems, a practice also known as 'shadow-banning', can be also considered as a moderation tool for its rationale (see *infra*: Chapter III).

¹²² Rasha Younes, 'Meta's Broken Promises' <<https://www.hrw.org/report/2023/12/21/metabroken-promises/systemic-censorship-palestine-content-instagram-and>> accessed 25 March 2025.

to it is heavily affected. The gatekeeping function here does not concern access per se, but rather the manipulation of content's visibility and potential reach.¹²³ While general prioritisation mechanisms have long existed in traditional media, such as placing a story on the front page or scheduling it during peak television hours, digital technologies have enormously amplified the capacity to personalise rankings based on individual users' preferences.¹²⁴ Tailored content recommendations are a particularly concerning dimension of platforms' opinion power, since microtargeting techniques significantly enhance their capacity to exert an effective influence on recipients, as further discussed below.

Concerning the impact of prioritisation on public opinion, empirical research has long demonstrated that the order in which information about elections and candidates appears in search results can shape voting preferences.¹²⁵ A very recent and striking example of the potential impact of content prioritisation on democratic processes has been the first-round victory of the ultranationalist and pro-Russian candidate Călin Georgescu in Romanian elections. The candidate was reportedly little known before a viral paid advertising campaign on TikTok (which was not labelled as political campaign). The unexpected result prompted a groundbreaking intervention by the Romanian Constitutional Court, which ultimately led to Georgescu's exclusion from the second round of voting.¹²⁶ Even though the precise

¹²³ Helberger, Kleinen-von Königslöw and Noll (n 4) 62.

¹²⁴ Helberger (n 80) 846.

¹²⁵ Nicholas Diakopoulos and others, 'I Vote For - How Search Informs Our Choice of Candidate' in Damian Tambini and Martin Moore, *Digital Dominance. The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018).

¹²⁶ Rowan Ings, 'Romanian Elections: TikTokers and an Election Scandal' (*BBC*, 29 April 2025) <<https://www.bbc.com/articles/cqx41x3gn5zo>> accessed 8 September 2025. This case led the European Commission to investigate into TikTok's compliance with the DSA and its systemic risks obligations. See: European Commission, 'Commission Opens Formal Proceedings against TikTok under DSA' (*European Commission*, 22 April 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487> accessed 8 September 2025. John Albert, 'TikTok and the Romanian Elections: A Stress Test for DSA Enforcement - DSA Observatory' (20 December 2024) <<https://dsa-observatory.eu/2024/12/20/tiktok-and-the-romanian-elections/>> accessed 8 September 2025. In the meanwhile, TikTok declared its commitment to protect the integrity of elections: TikTok, 'Continuing to Protect the Integrity of

causal link between content prioritisation and voting outcomes remains to be definitively established, the episode illustrates how disproportionate visibility can still undermine the perceived legitimacy of democratic competition. On the additional concerns raised by microtargeting techniques, the Cambridge Analytica scandal constitutes a prime example: the company harvested personal data from millions of Facebook users without their consent and used it to build detailed individual profiles, which were then exploited to deliver highly personalized political advertising and allegedly influencing elections, including the 2016 U.S. presidential race and the Brexit referendum.¹²⁷

Notably, these two cases, in which platforms were accused of influencing electoral outcomes, were not connected to their preference for one candidate over another. For this reason, the issue of platforms' opinion power does not necessarily stem from their will to promote a political agenda of their own. That said, there are instances where platforms have acted as 'direct speakers', as previously discussed; while other allegations of politically biased gatekeeping include claims of systematic suppression of conservative news in Facebook's the trending section,¹²⁸ and the apparent slowdown of progressive media websites on X.¹²⁹ Moreover, Elon Musk's public endorsement of Donald Trump's 2024 re-election bid marked a new

TikTok during Romanian Elections' (*Newsroom | TikTok*, 6 December 2024) <<https://newsroom.tiktok.com/continuing-to-protect-the-integrity-of-tiktok-during-romanian-elections?lang=en-150>> accessed 27 October 2025.

¹²⁷ Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, 'How Trump Consultants Exploited the Facebook Data of Millions' *The New York Times* (17 March 2018) <<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>> accessed 24 February 2025.

¹²⁸ Michael Nunez, 'Former Facebook Workers: We Routinely Suppressed Conservative News' (*Gizmodo*, 9 May 2016) <<https://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006>> accessed 25 March 2025.

¹²⁹ Jeremy B Merrill and Drew Harwell, 'Elon Musk's X Is Throttling Traffic to Websites He Dislikes' *The Washington Post* (15 August 2023) <<https://www.washingtonpost.com/technology/2023/08/15/twitter-x-links-delayed/>> accessed 25 March 2025.

era of intentional use of platforms' opinion power.¹³⁰ However, in most of cases, filtering activities have not been driven by ideological stances, but rather by commercial incentives.

Some further elaboration on digital platforms' business model is warranted here.¹³¹ Much like traditional media, digital platforms are often described as operating within a multi-sided market.¹³² On one side are the users, who access the service for free; on the other are advertisers, who pay to have their content shown. Advertising thus constitutes the primary revenue stream for most platforms. Importantly, the value of advertising space is determined by the platform's ability to reach an audience, both in quantitative and qualitative terms. Indeed, advertisers are interested in the sheer volume of users the platform can deliver; as well as in the precision with which those users can be targeted. Consequently, the more user attention platforms are able to offer advertisers, the higher the amount of advertising spent on their services. But in order to sell attention, platforms must first capture it. As a result, the content transmitted through their outlets must be as engaging as possible. This economic motivation to pursue viral spread leads to unintended consequences.¹³³ Recommender systems are personalised based on user data to maximise appeal, potentially resulting in harmful side effects for the democratic

¹³⁰ Le Monde, 'Le soutien problématique d'Elon Musk à Donald Trump' (22 October 2024) <https://www.lemonde.fr/idees/article/2024/10/22/le-soutien-problematique-d-elon-musk-a-donald-trump_6358082_3232.html> accessed 18 September 2025; Dan Primack and Scott Rosenberg, 'Tech Leaders Line up behind Trump' (*Axios*, 16 July 2024) <<https://www.axios.com/2024/07/16/andreesen-horowitz-musk-trump>> accessed 18 September 2025. Some considerations on this point can be found in: Julian Uhlenbusch, 'Elon Musk, the Systemic Risk' (*Verfassungsblog*, 7 February 2025) <<https://verfassungsblog.de/elon-musk-the-systemic-risk/>> accessed 7 February 2025; Paddy Leerssen, 'From Murdoch to Musk: Platform Ownership and the Political Economy of Online Content Governance' (2025) 2 *Platforms & Society* 29768624251386260 <<https://doi.org/10.1177/29768624251386260>> accessed 26 October 2025.

¹³¹ This topic is further discussed below in Chapter IV.

¹³² However, this conceptualisation is not universally accepted. For instance, Newman suggests a different model in which users are not simply one side of the market, but rather the producers – of attention – while digital intermediaries act as distributors, and advertisers are the true end clients. (Newman (n 26).)

¹³³ Cohen (n 3) 85.

debate, such as the promotion of extreme content,¹³⁴ or the creation of echo chambers.¹³⁵ This is because recommender systems values personal significance, whereas traditional news organisations emphasise social significance.¹³⁶ Subsequently, a portion of this communicative power is sold to the highest bidder, whether advertisers, governments, or political parties.¹³⁷ Once again, advertising is targeted based on the processing of personal data in order to enhance its effectiveness. This is the core logic of the so-called ‘attention economy’.¹³⁸ It is in this double transaction – attracting attention from users and selling it to advertisers – that the functioning of every recommender system is grounded. However, while this double transaction also characterises traditional media markets, the digital sector differs for its additional capacity of attracting attention through personalised content recommendations.

Another distinctive feature of digital platforms lies in the fact that their filtering activities are performed through algorithmic systems. These systems function simultaneously as tools for the automatic detection and removal of problematic content and as mechanisms for ranking, prioritising, and recommending information.¹³⁹ Search engines and social media platform services consist in algorithmically sorting information: in this sense, they *are* their algorithms. Although designed according to specific goals, such as maximising engagement, or complying with legal requirements, it is ultimately the algorithm that determines

¹³⁴ Dhiraj Murthy, ‘Evaluating Platform Accountability: Terrorist Content on YouTube’ (2021) 65 *American Behavioral Scientist* 800 <<https://doi.org/10.1177/0002764221989774>> accessed 7 January 2025.

¹³⁵ Eli Pariser, *Il Filtro* (Il Saggiatore 2012) <<https://www.ilsaggiatore.com/libro/il-filtro>> accessed 13 November 2024; Cass R Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (NED-New edition, Princeton University Press 2018) <<https://www.jstor.org/stable/j.ctv8xnhtd>> accessed 13 November 2024.

¹³⁶ Napoli (n 7) 63.

¹³⁷ Helberger (n 80) 846.

¹³⁸ Wu, ‘Is the First Amendment Obsolete?’ (n 114) 555.

¹³⁹ Gillespie (n 60) 181; Robert Gorwa, Reuben Binns and Christian Katzenbach, ‘Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance’ (2020) 7 *Big Data & Society* <<https://doi.org/10.1177/2053951719897945>> accessed 9 May 2025.

which content users encounter.¹⁴⁰ Most algorithms rely on machine-learning techniques that autonomously refine their selection criteria based on patterns extracted from vast quantities of data. This process includes the collection and analysis of personal data, used to predict which content an individual user is most likely to engage with and to generate targeted recommendations accordingly. In this sense, what distinguishes digital platforms' opinion power from that of traditional media is the knowledge and the technical tools to command online attention, which together grant platforms an unprecedented potential for persuasion.¹⁴¹

Whether the transmission of politically relevant content is shaped by the platforms' own political leanings, by their algorithmic pursuit of user engagement, or by the interests of the highest bidder, there is no guarantee that such transmission, even when not malicious or biased, aligns with the public interest.¹⁴² The core issue is that, regardless of the motivation, platforms retain the unilateral power to determine relevance, thereby setting the terms of public discourse. As Martin Moore put it:

*'When almost all our news is channelled through particular gateways then, as citizens, it is important that we are aware which information is filtered and why, as Google's definition of important, or accurate, or impartial, or relevant, news may be different from ours'.*¹⁴³

This concentration of gatekeeping power, exercised outside public scrutiny, has brought to the fore the need to adapt existing regulatory framework to the contemporary digital environment and its role within the information ecosystem. In this regard, the European Union has acted as a pioneer, as discussed in the following paragraph.

¹⁴⁰ Taina Bucher, 'Want to Be on the Top? Algorithmic Power and the Threat of Invisibility on Facebook' (2012) 14 *New Media & Society* 1164 <<https://doi.org/10.1177/1461444812440159>> accessed 21 November 2024.

¹⁴¹ Helberger (n 80) 846.

¹⁴² Moore (n 7) 34; A Diaz, 'Through the Google Goggles: Sociopolitical Bias in Search Engine Design' (2008).

¹⁴³ Moore (n 7) 33.

2.2. EXTENDING PUBLIC INTEREST REGULATION TO NEW INFORMATION INTERMEDIARIES

Since the early 2000s, scholars have acknowledged that regulating online platforms, and particularly search engines, is a political and democratic matter,¹⁴⁴ as they present the features of a new public space for democratic expression, a contemporary ‘Hyde Park corner’.¹⁴⁵ However, although these companies have often defended their nature of unregulated spaces,¹⁴⁶ they actually impose their own access rules, and there is no guarantee that these serve the public interest. Given their control over distribution channels and the magnitude of their audience, digital platforms have at times been compared to broadcasters.¹⁴⁷ As mentioned above, intermediation and distribution are inherently associated with a certain degree of power,¹⁴⁸ i.e. the power to select content. This is a classical problem of media regulation: no intermediary is naturally neutral or aligned with the public good; but such outcomes can only derive from regulatory frameworks designed to limit gatekeeping power. From this perspective, the acknowledgment of the civic role played by digital platforms makes it inevitable for democratic societies to seek to regulate them, particularly raising questions about whether some of the rules traditionally applied to media organisations should also extend to them.¹⁴⁹

Indeed, specific regulatory frameworks have historically applied to distribution actors within the communication sector. In the U.S. legal system, the special responsibilities borne by communication companies are commonly framed under

¹⁴⁴ Introna and Nissenbaum (n 24).

¹⁴⁵ Introna and Nissenbaum (n 24); Julian C York, ‘Policing Content in the Quasi-Public Sphere’ (*OpenNet Initiative*, 2010) <<https://opennet.net/policing-content-quasi-public-sphere>> accessed 23 December 2024.

¹⁴⁶ Moore (n 7) 20.

¹⁴⁷ Moore (n 7) 29. However, Tim Wu recalls that the golden age of television, ranging approximately from 1930s till the early 1990s, ‘*was the era of the true national mass media [...] unparalleled in history, when people in the same nation mostly watched and listened to the same information*’ (Wu, ‘Is Filtering Censorship? The Second Free Speech Tradition’ (n 1) 7.).

¹⁴⁸ Napoli (n 7) 59.

¹⁴⁹ Moore (n 7) 30.

the notion of ‘public interest regulations’.¹⁵⁰ An example concerns telephone companies, which are subject to strict non-discrimination requirements under their ‘common carrier’ obligations.¹⁵¹ These neutrality rules aim to prevent major intermediaries from distorting commerce or political discourse by virtue of their position.¹⁵² Similar principles had been extended to Internet Service Providers under the Obama administration, in light of their technical capacity to favour traffic directed to certain websites over others.¹⁵³ Additional examples of public interest regulation include the ‘must-carry’ obligations imposed on cable networks, which ensure the distribution of socially valuable yet less commercially attractive content, such as local news;¹⁵⁴ as well as the ‘fairness doctrine’, long applied to broadcasters to guarantee the exposure of audiences to a diversity of political viewpoints.¹⁵⁵

The need to limit concentration of power on single media entities and to safeguard diversity is also connected to specific and enhanced antitrust rules, particularly in the context of merger control.¹⁵⁶ Rules governing the distribution of political and electoral content are likewise widespread across democratic jurisdictions. These range from equal access obligations for political candidates, to outright bans on political advertising on broadcast television, labelling requirements for political content, and restrictions on campaign financing.¹⁵⁷ Moreover, many European countries have a long-standing tradition of public service broadcasting, premised on the idea that access to plural and reliable information is essential to democratic life.

¹⁵⁰ Philip Napoli and Robyn Caplan, *When Media Companies Insist They’re Not Media Companies and Why It Matters for Communications Policy* (2016) 18.

¹⁵¹ Wu, ‘Is Filtering Censorship? The Second Free Speech Tradition’ (n 1) 10; Pasquale (n 7) 491.

¹⁵² Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) 489 <<https://www.jstor.org/stable/j.ctt13x0hch>> accessed 10 June 2025.

¹⁵³ Napoli (n 7) 51.

¹⁵⁴ Pasquale (n 7) 491; Napoli (n 7) 60.

¹⁵⁵ Wu, ‘Is Filtering Censorship? The Second Free Speech Tradition’ (n 1) 11.

¹⁵⁶ Napoli and Caplan (n 150) 18.

¹⁵⁷ Tambini (n 7) 266.

Many of these regulatory measures were originally justified by technological scarcity (e.g., the limited spectrum available for over-the-air broadcasting),¹⁵⁸ a condition largely overcome by today's digital infrastructure. However, scholars have consistently argued that the concentration of distribution channels and the limited capacity of human attention pose analogous concerns.¹⁵⁹ In this regard, Herbert Simon predicted in 1971 that:

*'In an information-rich world, the wealth of information means [...] a scarcity of whatever it is that information consumes. What information consumes is rather obvious: it consumes the attention of its recipients. Hence a wealth of information creates a poverty of attention [...]'.*¹⁶⁰

Therefore, in the digital age, the core problem is no longer spectrum scarcity but the bottlenecks of attention and visibility, which make the regulation of platform gatekeeping power no less urgent. Indeed, irrespective of technological advancements, humans are only capable of processing a limited amount of information within a given period of time, making exposure to information more important than its mere availability.

While the necessity of regulating platforms' opinion power has long been acknowledged in academic debates, the issue only gained prominence on political agendas after the disruptive outcomes of the 2016 UK referendum and US presidential elections, which sparked widespread concerns over the role of social media in spreading disinformation.¹⁶¹ In this context, 'digital governance' became a priority for public authorities.¹⁶² The European Union has emerged as one of the most proactive global actors in this field, launching in 2020 a European Digital Strategy built on three pillars: a technology that works for people, a fair and

¹⁵⁸ Pasquale (n 7) 492.

¹⁵⁹ Wu, 'Is the First Amendment Obsolete?' (n 114) 554.

¹⁶⁰ Cited in: Wu, 'Is the First Amendment Obsolete?' (n 114) 554.

¹⁶¹ Tambini (n 7) 266.

¹⁶² Robert Gorwa, 'What Is Platform Governance?' (2019) 22 Information, Communication & Society 854, 4 <<https://doi.org/10.1080/1369118X.2019.1573914>> accessed 13 November 2024.

competitive digital economy, and an open, democratic, and sustainable society.¹⁶³ This strategy was among the priorities set by Ursula von der Leyen prior to her first nomination as President of the European Commission, reflecting her vision to create ‘a Europe fit for the digital age’.¹⁶⁴ In a broader sense, these initiatives reflected a path towards ‘digital constitutionalism’, meaning the effort to transpose constitutional values, fundamental rights, and democratic checks and balances into the a digital sphere where private corporations increasingly perform quasi-public functions.¹⁶⁵

Among the Strategy’s most significant initiatives is the Digital Services Act Package, which includes the Digital Services Act and the Digital Markets Act. The DSA, in particular, aims to enhance democratic control over the platform ecosystem and ensure greater accountability for how platforms exert their content curation practices. Notably, the DSA is also part of the European Democracy Action Plan,¹⁶⁶ one of whose main objectives is to adapt regulatory frameworks to the digital transformation of democratic life. While the DSA is the principal instrument addressing the role of online intermediaries on information flows, other regulations complement its approach, such as the Regulation on the Transparency and Targeting of Political Advertising, and the European Media Freedom Act. The Digital Markets Act, on its part, although primarily focused on promoting fair

¹⁶³ 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.

¹⁶⁴ von der Leyen (n 9).

¹⁶⁵ Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022) 1 <<https://www.cambridge.org/core/books/digital-constitutionalism-in-europe/A3F61C6368D17D953457234B8A59C502>> accessed 13 November 2024.

¹⁶⁶ Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan, 3.12.2020, COM/2020/790/final. Main information can be accessed here: European Commission, ‘Protecting Democracy’ (*European Commission*, 25 November 2021) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy_en> accessed 23 October 2025.

competition, indirectly affects platforms' opinion power by limiting their unilateral rule-making capacity over the functioning of their infrastructure. Moreover, since content curation on platforms is mainly performed through machine-learning algorithmic systems, the AI Act, representing the European pioneering effort to regulate emerging risks related to the dissemination of AI systems, is also relevant in this context.

Despite the first von der Leyen Commission's success in adopting several ambitious regulatory frameworks for the digital sector aimed at promoting European values, the second mandate appears to be marked by a prevailing deregulatory sentiment.¹⁶⁷ The growing normative density of EU law has increasingly been criticised for allegedly hindering the competitiveness of European markets, both by limiting access for non-European companies and by constraining the emergence of European ones. This argument has been prominently advanced within the Draghi Agenda and in Enrico Letta's report on the Single Market.¹⁶⁸ While excessive regulatory complexity may indeed create inefficiencies, and greater coherence and rationalisation is needed,¹⁶⁹ simplification should primarily aim to strengthen the protection of European values and fundamental rights,¹⁷⁰ fostering the anthropocentric vision supporting recent digital regulations.

¹⁶⁷ Euractiv, 'The Language of EUconomics' (*Euractiv*, 4 October 2025) <<https://www.euractiv.com/news/the-secrets-of-eurospeak/>> accessed 22 October 2025. Wax (n 11).

¹⁶⁸ Mario Draghi, 'The Future of European Competitiveness' (European Commission 2024) <https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en>; Enrico Letta, 'Much More than a Market. Speed, Security, and Solidarity. Empowering the Single Market to Deliver a Sustainable Future and Prosperity for All EU Citizens' (2024) <<https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf>>. European Commission, 'The Draghi Report on EU Competitiveness' (*European Commission*) <https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en> accessed 23 October 2025; 'Enrico Letta's Report on the Future of the Single Market - Internal Market, Industry, Entrepreneurship and SMEs' <https://single-market-economy.ec.europa.eu/news/enrico-lettas-report-future-single-market-2024-04-10_en> accessed 23 October 2025.

¹⁶⁹ See *infra*: Chapter V.

¹⁷⁰ Pollicino (n 11).

Furthermore, geopolitical tensions following the re-election of Donald Trump as President of the United States have further weakened consensus on digital services regulations, as his administration chose to firmly defend the interest of US Big Tech,¹⁷¹ threatening the imposition of higher tariffs in response to European enforcement measures.¹⁷² Overall, the political momentum that once sustained digital constitutionalism in Europe appears to be fading. This shift could have a tangible impact on both the enforcement of existing frameworks and the likelihood of further regulatory initiatives in the digital sphere.

CONCLUDING REMARKS

Digital platforms have been defined as online services that enable the upload and public transmission of information. They therefore fall within the broader category of intermediaries, as they do not produce their own content but rather facilitate interactions between third parties. In this capacity, they serve as enablers, contributing to the democratisation of content production and dissemination. However, today's economic and social life is dominated by a small number of major digital platforms that control the vast majority of online markets' shares. This concentration means that global communications are intermediated by a few private actors acting as gatekeepers, a notion associated with the power derived from the ownership of essential infrastructures.

¹⁷¹ Anna Vicinanza, 'Il primo atto di enforcement del Digital Services Act tra tensioni geopolitiche: la sanzione della Commissione europea nei confronti di X (Twitter) – AISDUE' (*Blog DUE*, 18 January 2026) <<https://www.aisdue.eu/anna-vicinanza-il-primo-atto-di-enforcement-del-digital-services-act-tra-tensioni-geopolitiche-la-sanzione-della-commissione-europea-nei-confronti-di-x-twitter/>> accessed 5 February 2026.

¹⁷² 'Lutnick Says EU Must Change Digital Rules for Steel Tariff Deal' *Bloomberg.com* (24 November 2025) <<https://www.bloomberg.com/news/articles/2025-11-24/lutnick-says-eu-must-change-digital-rules-for-steel-tariff-deal>> accessed 5 February 2026. The U.S. administration has recently escalated this tension by imposing travel restrictions on individuals involved in technology regulation, including former EU Commissioner Thierry Breton.: 'Former EU Commissioner and Activists Barred from US in Attack on European Tech Regulators' *The Guardian* (24 December 2025) <<https://www.theguardian.com/technology/2025/dec/24/us-state-department-visa-ban-former-eu-commissioner-europe>> accessed 5 February 2026.

Platforms are not only essential infrastructures for commercial exchanges but also for the circulation of political and publicly relevant information. The gatekeeping of information flows translates into opinion power, which is inherently connected to the distribution of political power and the functioning of democratic processes. The capacity of platforms to influence public opinion derives from their filtering activities: they can hinder the transmission of certain information while amplifying the visibility of others. These practices are carried out through moderation and prioritisation practices, largely based on algorithmic processes. Several examples have illustrated the significance of such practices for public discourse, including the systematic demotion of news related to Gaza and the disproportionate visibility given to a pro-Russian candidate during the recent Romanian elections. However, it has also been argued that moderation and prioritisation mechanisms are generally driven not by platforms' specific political interests but by commercial incentives aimed at maximising time spent by users on these services.

At the same time, the digital landscape has recently seen the emergence of new information distributors, notably generative AI systems such as ChatGPT and Google Gemini, which are increasingly used to access content online. Unlike traditional digital platforms, their classification as intermediaries is debatable. Although their functioning relies on third-party material, these systems generate new content rather than merely transmitting existing information. Nevertheless, they also exercise gatekeeping power: they exclude certain perspectives from their outputs (moderation) and determine which information is selected and reformulated (prioritisation). While this research focuses on digital platforms, some considerations on the regulation of these other actors is presented.

Gatekeeping power over politically relevant information has traditionally characterised communications industries, such as broadcasters or telephone companies. The need to align the use of these technologies with the public interest has often prompted the adoption of substantial sector-specific regulation, whose extension to the digital sector has been debated. Recent EU initiatives, adopted with

the broader aim of aligning the governance of digital spaces with European values, can be interpreted as an attempt to introduce public interest considerations into platforms' unilateral content curation practices. However, the merit of these new regulatory efforts has been increasingly challenged by a concurrent political trend favouring instead deregulation. The main provisions introduced by these instruments are analysed in the following chapters, with the aim of assessing how the European Union has sought to counterbalance and limit the opinion power of digital platforms.

Since the regulation of digital intermediaries has traditionally been approached through the lens of their liability for third-party content, this is the first issue addressed in the present research. This question is particularly relevant because liability rules determine whether platforms are required to exert control over the content they transmit (i.e., they must actively play their gatekeeping role), or whether they may remain neutral conduits of information. Traditionally, EU and US regulations adopted a laissez-faire, self-regulatory model: platforms were under no obligation to monitor user content but retained full discretion to remove or restrict it at will. In either case, they were exempt from responsibility for the outcome. As shown in the following chapter, the Digital Services Act have introduced significant innovations on this topic.

II. INTERMEDIARIES' LIABILITY FOR THIRD-PARTY ILLEGAL CONTENT AND DUTIES TO ACT

This chapter examines platform liability for hosting illegal content generated by third parties. Due to their intermediary role, platforms typically do not create their own content and are therefore rarely subject to direct or primary liability.¹⁷³ However, liability is traditionally linked not only to content production but also to its distribution.¹⁷⁴ This gives rise to secondary liability, which can take various forms – civil, criminal, or administrative.¹⁷⁵ Indeed, many legal systems recognise secondary liability for editorial curation, based on the principle that those who control publishing decisions should be held responsible for the content they select, even if it originates from a third party. Just as publishers, by selecting what to publish, bear responsibility for their content, platforms that curate or suppress user-generated content could similarly face liability for illegal material. However, this approach raises significant concerns regarding platforms' influence on public opinion and users' rights, since imposing a broad obligation to monitor communications could lead platforms to adopt overly cautious content moderation policies, resulting in unnecessary restrictions and negatively impacting freedom of expression.

The issue of platforms' liability is also closely tied to the need to strike a balance between fostering legality in the digital environment and safeguarding fundamental rights. On the one hand, an absolute prioritisation of legality would entail the imposition of stringent control obligations on platforms, triggering their liability. This would prompt them to expeditiously remove any illegal content. Indeed, the

¹⁷³ However, a primary liability could arise when the platform actively contributes to illegality through positive actions. This could occur not only when the platform itself generates content but also when it prioritizes it. This issue will be further explored in the next chapter.

¹⁷⁴ Napoli (n 7) 7.

¹⁷⁵ Andrea Bertolini, Francesca Episcopo and Nicoleta-Angela Cherciu, 'Liability of Online Platforms' (European Parliamentary Research Service 2021) PE 656.318 26.

stricter the liability, the more likely it is that content will be removed.¹⁷⁶ Conversely, freedom of expression would be maximised if platforms were prohibited from exercising any form of control over user-generated content. This would imply imposing them a form of neutrality and a obligation to provide free access.

These considerations have roots as old as the World Wide Web itself. The question of whether platforms should bear any responsibility for illegal content and, specifically, whether they have an obligation to moderate it and can be held liable for failing to do so, has been addressed since the 1990s. However, as the structure of the web has evolved, the debate has resurfaced, prompting renewed debates and some reforms.

The first part of this chapter (Section 1) outlines the traditional framework for intermediary liability, comparing the approaches in the US and the EU, and examining the interpretative challenges that have emerged with the evolution of the online landscape. In the EU, these challenges have led to the adoption of a new regulatory framework, the Digital Services Act, whose provisions affecting intermediary liability are analysed in the second part of this chapter (Section 2).

1. FROM SAFE HARBOUR TO DEMANDS FOR ACCOUNTABILITY

The traditional western regulation of online intermediaries provides a general exemption of liability in favour of digital service providers for content transmitted on the behalf of third parties. This solution, adopted in the United States, in the EU and in many other legal systems, allegedly reflects a pro-freedom of expression perspective, through the creation of the so-called *safe harbour*.¹⁷⁷ However, this regime has come under increasing pressure due to the evolution of the digital

¹⁷⁶ This is true also in a practical sense: studies have shown that in countries where the liability is stricter, freedom of expression online is lower (Rebecca MacKinnon and others, 'Fostering Freedom Online: The Role of Internet Intermediaries' 30.).

¹⁷⁷ Pasquale (n 7) 494.

landscape and the growing centrality of online platforms, which no longer fit neatly within the early-2000s conception of intermediary services. After presenting the safe harbour regulatory frameworks (Section 1.1), the notion of intermediary service and its contested neutrality, which should represent the rationale for immunity, is examined (Section 1.2), followed by an overview of the first shifts towards enhanced responsibility within the EU legal system (Section 1.3).

1.1. SAFE HARBOUR: INTERMEDIARIES' LIABILITY EXEMPTIONS IN THE US AND EU LEGAL SYSTEMS

The US safe harbour regulation is famously based on the Section 230 of the 1996 Communication Decency Act (CDA), which contains two statements: (i) providers of an 'interactive computer service'¹⁷⁸ must not be treated as publishers or speakers of information provided by other users; (ii) civil liability of providers taking voluntary actions to restrict access to 'objectionable' material is excluded.

The first part of Section 230 provides a general liability exemption for platforms hosting illegal content generated by third parties. The exemption applies both to primary liability (as a 'speaker'), and secondary liability (as an 'editor').¹⁷⁹ This rule serves multiple purposes: it was mainly designed to prevent government censorship online and to preserve the Internet as a space for free expression.¹⁸⁰ At the same time, it aimed to incentivise market development, as doubts about the technical feasibility of a pervasive content control and corresponding risks of failure could hinder economic actors to enter the market and restrain innovation.¹⁸¹

¹⁷⁸ This definition will be further discussed below.

¹⁷⁹ Bertolini, Episcopo and Cherciu (n 175) 26.

¹⁸⁰ Giovanni Sartor, 'The Secondary Liability of Online Intermediaries' in Pier Luigi Parcu and Elda Brogi (eds), *Research Handbook on EU Media Law and Policy* (Edward Elgar Publishing 2022) 151. Giancarlo Frosio and Christophe Geiger, 'Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime' (2021) 29 *European Law Journal* 31, 34 <<https://papers.ssrn.com/abstract=3747756>> accessed 13 November 2024.

¹⁸¹ Gillespie (n 60) 32. See also: Adam Thierer, 'Celebrating 20 Years of Internet Free Speech & Free Exchange' (*Medium*, 21 June 2017) <<https://readplaintext.com/celebrating-20-years-of-internet-free-speech-free-exchange-8a10f236d0bd>> accessed 13 March 2025. Barbara Ortutay, 'All

However, this protection only applies to civil liability and does not extend to federal criminal law and intellectual property violations. The relevant framework for copyright violations is instead the Digital Millennium Copyright Act (DMCA),¹⁸² which shields online service providers from liability for hosting infringing material only if they promptly remove or disable access to the content upon receiving a notification by the rights holder. This creates a form of ‘conditional liability’ based on a notice-and-takedown mechanism, bringing this US sectorial framework closer to the approach later adopted within the EU through the Electronic-Commerce Directive,¹⁸³ as described below.

The second part of Section 230, commonly referred to as the ‘*Good Samaritan Protection*’, is based on the premise that platforms should not face legal repercussions for spontaneously removing harmful or illegal content, when acting in good faith. More precisely, it allows platforms to remove content they consider ‘*obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable*’, even if the material is constitutionally protected. This provision ensures that content moderation does not reclassify platforms as publishers or speakers, thereby preserving their liability exemption. Its goal is then to encourage platforms to exercise some degree of control over content and combat the dissemination of harmful material through self-regulation.¹⁸⁴ By establishing a right, rather than an obligation, to delete content, this provision promotes proactive moderation.¹⁸⁵

about Section 230, a Rule That Made the Modern Internet’ (*AP News*, 28 May 2020) <<https://apnews.com/article/d3e09c4037e2fc17558492b9bdce1ecc>> accessed 13 March 2025.

¹⁸² The Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998), Title II, adding a new Section 512 to the Copyright Act.

¹⁸³ Sartor (n 180) 152.

¹⁸⁴ De Gregorio (n 165) 42.

¹⁸⁵ Gillespie (n 60) 31.

As a result, under the US framework, platforms have full discretion over whether to engage in moderation and what type of content to restrict. The decision to intervene – or not – is entirely left to the platform’s will and remains detached from any form of legal scrutiny or responsibility. Accordingly, the balance between legality and freedom of expression is entirely entrusted to private platforms, as the system does not incorporate any public interest consideration. There is no guarantee that either legality or freedom of speech are safeguarded. In fact, platforms may choose to remove lawful content while retaining illegal content. While this model protects users’ freedom of expression in its vertical dimension (i.e., protection from state interference), it fails to address its horizontal dimension, as platforms are under no obligation to safeguard it.

The European Union regulation came four years after Section 230 with the adoption of the Electronic Commerce Directive (‘ECD’).¹⁸⁶ While based on a similar exemption principle, it contains several differences. Notably, it is said to create a *conditional* liability exemption, rather than a *pure* exemption as in the United States legal system.¹⁸⁷ Specifically, Articles 12, 13 and 14 of the ECD state that online intermediary service providers are not liable for the information they transmit or store at the request of users, but only if they meet certain conditions. These conditions are intended to ensure that the provider genuinely acts as an intermediary, namely it does not produce or modify the content, nor it is aware of its unlawfulness.

¹⁸⁶ 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 (‘Directive on electronic commerce’)

¹⁸⁷ MacKinnon and others (n 176) 50.

The ECD applies to ‘information society services’, defined by Directive 98/34/EC, as amended by Directive 98/48/CE.¹⁸⁸ These are ‘*services provided at a distance, by means of electronic equipment, for the processing and storage of data, and at the individual request of a recipient*’. The preamble of the ECD clarifies that this definition includes services that are not remunerated, provided they constitute an economic activity, including tools for searching and accessing data, as well as for the transmission of information through communication networks.¹⁸⁹

Liability rules, set out in Section 4, specifically apply to information society services that perform an intermediary role. The preamble helps defining intermediation, stating that liability exemptions apply only to activities performed by service providers to grant access to a network, when they are limited to a ‘*technical process [...] for the sole purpose of making the transmission more efficient*’.¹⁹⁰ Such activity must be merely ‘*technical, automatic and passive*’, meaning that the provider has neither knowledge nor control over the information.¹⁹¹ This statement raises the additional issue of defining *passivity*, which became particularly problematic for intermediaries qualifying as hosting providers,¹⁹² given the emergence of digital platforms widely relying on content curation practices. For this reason, this part of the preamble has been repeatedly addressed by the Court of Justice, as further analysed below (1.2).

Under the ECD, the conditions for benefiting from the liability exemption depend on the type of intermediary service provided. The Directive identifies three categories of intermediary services: *mere conduit* (Article 12), *caching* (Article 13), and *hosting* (Article 14). These categories are distinguished primarily by the type

¹⁸⁸ Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, Article 1(2).

¹⁸⁹ ECD, Recital 18.

¹⁹⁰ ECD, Recital 42.

¹⁹¹ ECD, Recital 42..

¹⁹² Bertolini, Episcopo and Cherciu (n 175) 29.

and duration of user information storage involved. Mere conduit refers to services such as Wi-Fi access points or mobile broadband, which are based on a storage of user content which is automatic, intermediate and ‘transient’, i.e. limited for the time necessary to the transmission. Caching is similar to mere conduit, but storage is ‘temporary’ rather than transient, suggesting a longer duration. Conversely, hosting involves ‘storage’ as its core activity, without time constraints.¹⁹³

Since major platforms qualify as hosting services, special attention will be given to the conditions set out in Article 14. Indeed, the Court of Justice has classified search engines, social media platforms, and marketplaces as ‘hosting’ services,¹⁹⁴ and it is particularly in this context that its jurisprudence has evolved. Two conditions must be met for a hosting service to qualify for liability exemption: (a) it must not have actual knowledge of the illegal activity or information, or of the facts from which the illegality is apparent¹⁹⁵ (b) upon obtaining such knowledge, it must act expeditiously to remove or disable access to the information.

In this context the Directive also specifies that, in accordance with Member States’ legal system, national authorities may require service providers to terminate or prevent an infringement.¹⁹⁶ At the same time, Member States are prevented from

¹⁹³ Contrary to mere conduit and caching services, distribution activity is not explicitly mentioned by the provision concerning hosting services. However, it is generally acknowledged that the distribution function is inherent to storage, meaning that the provider stores an information with the aim to deliver it on users’ demand (Joris van Hoboken et al., *Hosting Intermediary Services and Illegal Content Online: An Analysis of the Scope of Article 14 ECD in Light of Developments in the Online Service Landscape: Final Report*, Directorate-General for Communications Networks, Content and Technology (European Commission) (Publications Office of the European Union, 2019), 12, <https://data.europa.eu/doi/10.2759/284542>).

¹⁹⁴ See *infra* for a detailed review of the Court of Justice jurisprudence concerning ECD application to online platforms. However, some remained outside this definition, and were therefore not covered by ECD exemption. This was the case for Uber, considered a transportation service and not an information service (Hoboken and others (n 193) 30.).

¹⁹⁵ This provision includes two types of consciousness: actual knowledge and constructive knowledge, i.e. awareness of facts (Hoboken and others (n 193) 29.).

¹⁹⁶ ECD, Article 14(3). Recital 45 states: ‘The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring

imposing on providers a general monitor obligation concerning the information transmitted or stored.¹⁹⁷ It follows that intermediaries do not have a general obligation to monitor content transmitted on behalf of third parties, but may be obliged to act with regard to content specifically identified by the competent national authorities. The possibility for national authorities to issue takedown orders for certain illegal content has been the subject of some rulings by the Court of Justice, particularly on the definition of the boundaries between specific (authorised) takedown orders and generalised (prohibited) surveillance obligations.¹⁹⁸ Furthermore, the Directive specifies that Member States may establish an obligation on providers to inform public authorities about alleged illegal activities of their users (in the event they become aware of them) or to communicate, upon request, information enabling the identification of specific users.

At this point, it can be noted that the liability exemption established by the ECD was significantly reduced in scope compared to the one existing in the United States. First, while Section 230 applies to any ‘interactive service’, meaning any service which allows third parties to upload content, the ECD only covered intermediary considered sufficiently ‘neutral’ or ‘passive’. Secondly, under the ECD the knowledge of the illegality implied the loss of the exemption. This means that a notice-and-take-down mechanism had been established,¹⁹⁹ whereby a notification about the illegality, both coming from public authorities or from privates, could trigger the provider’s liability.²⁰⁰ Finally, the ECD did not contain an explicit Good Samaritan provision to regulate spontaneous monitoring and

the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.’

¹⁹⁷ ECD, Article 15.

¹⁹⁸ See *infra*: Section 1.2.

¹⁹⁹ Hoboken and others (n 193) 27.

²⁰⁰ The Court of Justice of the European Union has ruled on this issue, as discussed below in Section 2.3.

removal of illegal activities, even though its preamble stated that the Directive should not prevent providers from taking measures against illegal content, whether upon injunction or spontaneously, and from developing technical systems of surveillance and control.²⁰¹ The absence of an explicit Good Samaritan clause had been criticised, accused of leaving a vacuum in the legislation.²⁰² Without such a clause, a provider proactively seeking and removing illegal or harmful content risks losing the classification of intermediary, and thus the liability exemption. This legal uncertainty, which entrenches with the issue of defining a ‘passive’ intermediary, could discouraged platforms from voluntarily removing unlawful content. Nonetheless, the Good Samaritan has come to be broadly recognised under EU law, supported by the jurisprudence of the Court of Justice,²⁰³ and certain official EU documents.²⁰⁴

Irrespective of the differences between the United States’ and the European Union’s specific frameworks, the principle of liability exemption has come under increasing scrutiny as the web’s structure has evolved. This shift is largely attributable to the widespread diffusion of platform services that engage in a broad range of content curation practices. As these platforms exercise growing influence over the selection, ranking, and dissemination of content, it has become increasingly difficult to regard them as neutral intermediaries merely facilitating communication between users. Rather, their role begun to increasingly resemble to that of traditional media entities, which actively shape public discourse through editorial choices. These developments have questioned the continued justification for

²⁰¹ ECD, Recital 40.

²⁰² Hoboken and others (n 193) 7.

²⁰³ As examined in the following paragraph.

²⁰⁴ European Commission’s Recommendation on illegal content in 2018, Recital 26. See: Folkert Wilman, ‘Between Preservation and Clarification. The Evolution of the DSA’s Liability Rules in Light of the CJEU’s Case Law.’ in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023) 44.

immunity and the need for regulatory reform. The following section examines how these debates have unfolded, particularly within the European legal context.

1.2. QUESTIONING SAFE HARBOUR: ARE ONLINE PLATFORMS MERE INTERMEDIARIES?

The platformisation of the web has placed increasing strain on the traditional safe harbour model for intermediary liability. Within the EU legal framework, much of the debate has centred on the definition of ‘intermediary service’, which serves as the precondition for benefiting from liability exemptions and has been largely anchored in the idea of ‘passivity’. This concept has been the subject of significant jurisprudence by the Court of Justice of the European Union, which has generally upheld the application of immunity despite evolving content curation practices by digital platforms. The section first reviews the Court’s approach, before turning to the wider academic, judicial and political debates, shared on both sides of the Atlantic, questioning the continued appropriateness of the safe harbour model in the context of increasingly interventionist platform services.

Over time, the Court of Justice has developed a jurisprudence regarding the ‘passive’ character of online platforms based on the ECD. While this criterion has been set aside by the Digital Services Act, which no longer requires passivity to define hosting services,²⁰⁵ a brief overview of the earlier jurisprudence remains useful, as it highlights many of the issues related to platform intervention on user-generated content. The relevant case-law has mostly concerned intellectual and industrial property rights. In *Google France v. Louis Vuitton* (2010),²⁰⁶ the Court ruled on Google’s potential liability for advertising third-party products infringing trademark rights. Through its ‘AdWords’ service, Google had been found sponsoring, for a fee, advertisements of counterfeit goods linked to keywords that

²⁰⁵ See *infra*: Section 2.

²⁰⁶ *Google France SARL and Google Inc v Louis Vuitton Malletier SA* [2010] Court of Justice of the European Union ECLI:EU:C:2010:159, C-236/08 to C-238/08.

included the claimant's brand name, raising the question of its liability. Since the tag-matching was performed automatically according to the advertiser's request, the requirement of lack of knowledge and control by the intermediary was considered satisfied by the Court. Moreover, the order of appearance of the advertisements was determined essentially by the amount paid by advertisers, following a common e-commerce pattern (i.e., more money is equal to more visibility). The Court held that ranking against payment did not deprive the platform of the 'passive' role referred to in Recital 42 of the ECD. Accordingly, the liability exemption under Article 14(1) of the ECD could apply. It is noteworthy that the Court's judgement diverged from the opinion of Advocate General Maduro, who considered AdWords to fall outside the scope of article 14 ECD, missing the condition of passivity.²⁰⁷ The Advocate General drew a distinction between Google's different services, namely Google Search and AdWords. In the first context, the platform displayed results automatically on the basis of neutral parameters such as popularity and relevance, with no self-interest involved. By contrast, with AdWords, Google shared an economic interest with advertisers, receiving greater remuneration when users clicked on their links. This implied that, in the latter case, Google was not hosting or transmitting information in a neutral manner and therefore should not benefit from intermediary liability shield.

Shortly after, in *L'Oréal vs. eBay* (2011),²⁰⁸ the Court confirmed the reasoning, arriving yet to an opposite solution.²⁰⁹ The facts were similar: the well-known 'eBay' marketplace hosted a number of products allegedly infringing the claimant's trademark. In this case, however, it was the intermediary itself (eBay) that selected keywords to promote third-party products through AdWords. Holding that the

²⁰⁷ *Google France SARL and Google Inc v Louis Vuitton Malletier SA* [2009] Opinion Of Advocate General Poiares Maduro ECLI:EU:C:2009:569, C-236/08, C-237/08 and C-238/08 §137-146.

²⁰⁸ *L'Oréal SA and Others v eBay International AG and Others* [2011] Court of Justice of the European Union ECLI:EU:C:2011:474, C-324/09.

²⁰⁹ CJEU, *L'Oréal* (n 208), §113.

requirement for immunity lies in the exclusive use of automated tools to process data in a technical way, the Court stated that an intermediary could not be considered neutral when its activities extend to facilitating relationships among users and to providing assistance in selling and sponsoring user products.²¹⁰ In such circumstances, the service provider is deemed to play an active role and therefore falls outside the scope of the liability exemption established by Article 14(1) ECD. Importantly, such reasoning was strongly contradicted by the Advocate General Jääskinen,²¹¹ who argued that Recital 42 of the ECD applied only to mere conduit and caching services, but not to hosting intermediaries, which instead fell under the scope of Recital 46.²¹² According to this interpretation, the active/passive dichotomy was irrelevant for determining the applicability of the liability exemption for hosting providers, as relying on such a distinction would endanger the objectives of the Directive. Furthermore, he argued that activities such as advising clients on how to draft advertisements and monitoring the content of listings should fall within the scope of the Good Samaritan protection.

Shortly thereafter, in *Scarlet*²¹³ and *Netlog*²¹⁴ cases, the Court addressed the issue of general monitoring obligation over users' content. The *Scarlet* case arose from a Belgian court order requiring an Internet Service Provider (ISP) to install a filtering system on all electronic communication among its users to prevent copyright infringements. The Court found this measure to violate Article 15 of the ECD, which prohibits the imposition of general monitoring obligations.²¹⁵ It ruled that intellectual property must be balanced against other fundamental rights.²¹⁶ In this

²¹⁰ CJEU, *L'Oréal* (n 208), §123.

²¹¹ *L'Oréal SA and Others v eBay International AG and Others* [2010] Opinion of Advocate General Jääskinen ECLI:EU:C:2010:757, C-324/09 §130-168.

²¹² Recital 46 should instead be the one deputy to apply to hosting intermediaries.

²¹³ *Scarlet Extended SA v Sabam* [2011] Court of Justice of the European Union ECLI:EU:C:2011:771, C-70/10.

²¹⁴ *Sabam v Netlog* [2012] Court of Justice of the European Union ECLI:EU:C:2012:85, C-360/10.

²¹⁵ CJEU, *Scarlet* (n 213), §40.

²¹⁶ CJEU, *Scarlet* (n 213), §44.

case, enforcing an automatic filtering mechanism would unduly have harmed users' rights, particularly the right to data protection and the right to information. It would equally be inconsistent with freedom of enterprise, provided that it would impose an excessive burden on the ISP, which was required to install a 'complicated, costly, permanent computer systems at its own expense'.²¹⁷ In summary, while national authorities are not precluded from issuing injunctions to internet providers in order to stop specific copyright infringements, as established in precedent case law,²¹⁸ such measures must not extend to imposing a general filtering system for all users without temporal constraints. The *Netlog* case was very similar, but involving a social network, and the Court came to the same conclusion.²¹⁹

In the *Facebook* case (2019), the Court ruled again on requests by public authorities to block illegal content, holding that the imposition of an automatic filtering mechanism is legitimate, provided that the request is sufficiently specific in nature.²²⁰ The preliminary ruling stems from a case concerning defamatory content shared on the platform against a member of an Austrian party, which the platform had refused to suppress, resulting in a proceeding before the commercial court in Vienna. While imposing a general monitoring would alter the intermediary's role, requiring a specific monitoring through automatic mechanisms to prevent substantially equivalent content from being shared again (i.e., with the same message and involving the same person) have been considered possible. This regards not only identical content, which was already declared illegal by a national court, but also content that 'whilst essentially conveying the same message, is worded slightly differently'.²²¹ However, the CJEU stated that such an injunction must not impose an excessive obligation on the host provider. This means that the

²¹⁷ CJEU, *Scarlet* (n 213), §46.

²¹⁸ CJEU, *L'Oréal* (n 208), §126-144.

²¹⁹ CJEU, *Netlog* (n 214), §47-52.

²²⁰ *Eva Glawischnig-Piesczek v Facebook Ireland Limited* [2019] Court of Justice of the European Union ECLI:EU:C:2019:821, C-18/18 §34.

²²¹ CJEU, *Facebook* (n 220), §41.

equivalent content must be precisely identified in order to not require the provider to carry out an independent assessment. In his opinion, the advocate general Szpunar underlined how imposing a general monitoring obligation would have altered the intermediary's role of hosting provider, which would lose its neutrality and, consequently, its liability exemption.²²² In fact, it would become aware of all the information stored or, even if this is not the case, it would be considered as to have such as knowledge and be held liable. On the contrary, specific monitoring obligations, if sufficiently precise, may be carried out automatically with the help of software tools, also implying a minor restriction of freedom of speech and privacy.²²³

In the *YouTube and Cyando* case (2021), the Court of Justice once again addressed the liability of hosting provider for copyright infringements occurring on their platforms, largely confirming previous jurisprudence.²²⁴ One of the questions referred for a preliminary ruling concerned the application of Article 14 of the ECD, and, specifically, the qualification of YouTube as intermediary provider. This qualification depends on the requirements of providing a merely 'technical, automatic, and passive' service, and not having 'knowledge nor control' over the information which it transmits. On this point, the Court clarified that the mere fact that a video-sharing platform, such as YouTube, voluntarily implements technological measures aimed at detecting certain illegal content does not, in itself, mean that the operator plays an active role, and may still qualify as an intermediary provider under the ECD.²²⁵ This statement can be read as a renewed confirmation

²²² *Eva Glawischnig-Piesczek v Facebook Ireland Limited* [2019] Opinion of Advocate General Szpunar ECLI:EU:C:2019:458, C-18/18 §36.

²²³ Opinion of Advocate General Szpunar (n 222), §61. However, in contrast with the Court, the Advocate General considered that monitoring obligations on equivalent content carried out towards all users are inconsistent with Article 15 of the ECD and unduly detrimental of individuals' rights.

²²⁴ *YouTube and Cyando* [2021] Court of Justice of the European Union ECLI:EU:C:2021:503, C-682/18 and C-683/18.

²²⁵ CJEU, *YouTube*, §109.

of a Good Samaritan-like protection in EU law under the ECD framework.²²⁶ The Court also addressed the relevance of ranking and recommendation systems in determining liability. Specifically, it analysed these elements in lights of the conditions established by Article 14 of the ECD, requiring the lack of knowledge of the illegal content in order to benefit from the liability exemption. It held that the fact that a platform automatically indexes uploaded content, offers a search function, and recommends videos based on users' preferences does not necessarily mean that it has *specific* knowledge of illegal content.²²⁷ Consequently, these practices do not affect the application of the liability exemption. More broadly, the Court also ruled out the liability for copyright infringements under the Directive 2001/29, holding that hosting providers do not, in principle, directly carry out 'acts of communications' within the meaning of Article 3 of the Directive. Instead, they merely provide the tool through which such communication may occur, thereby acting as intermediaries.²²⁸ In this regard, the Advocate General's opinion highlighted that, although the two legal tests (under the ECD and under Directive 2001/29) do not fully overlap, both hinge on the type of the provider's involvement: an intermediary may be considered as 'communicating to the public' if it intervenes actively in the act of communication (e.g., by retransmitting the content to a new audience or by transmitting its own content).²²⁹ In conclusion, the Court of Justice reaffirmed many of its earlier principles, confirming that YouTube is eligible to benefit from the liability exemption for hosting providers, despite engaging in various content curation and recommendation practices.

²²⁶ Wilman (n 204) 44.

²²⁷ CJEU, *YouTube*, §114.

²²⁸ Giacomo Bertelli and Jacopo Raposio, 'ISP Liability: Are Platforms like YouTube Directly Liable for Illegal Uploads?' (*MediaLaws*, 15 September 2020) <<https://www.medialaws.eu/isp-liability-are-platforms-like-youtube-directly-liable-for-illegal-uploads/>> accessed 14 May 2025.

²²⁹ *YouTube and Cyando* [2020] Opinion of Advocate General Saugmandsgaard Øe ECLI:EU:C:2020:586, C-682/18 and C-683/18 §75.

This jurisprudence by the Court of Justice, which has broadly upheld the liability shield even in the presence of content curation practices, has been subject to criticism from a variety of perspectives. The fact that platforms might be considered immune even when economically benefiting from illegal content, as in the case of Google France, has been criticised precisely for favouring Google's economic interests and for uncritically endorsing the platforms' business model with the purpose to preserve it.²³⁰ Another critical issue in the judgement regarded the classification of ranking activities. In this decision, the Court endorsed a perfect coincidence between automation, passivity and lack of knowledge.²³¹ However, scholars have highlighted the contradiction within the current system, given that generalized user monitoring through profiling is precisely the business model on which all these platforms are based.²³² In fact, platforms are perfectly able to identify users and intervene in their capacity to receive and transmit information,²³³ and they already exercise this capability, which contradicts arguments against imposing excessive obligations on platforms to avoid disrupting their business model. This situation has been referred to as the 'Good Samaritan paradox',²³⁴ meaning that the systematic filtering of information by platforms renders the claim of lack of knowledge a sort of legal fiction, creating a pure liability shield.

While safe harbour regulations are generally regarded as having promoted freedom to receive and impart information and ideas,²³⁵ as well as the development of platform digital market,²³⁶ they have increasingly been viewed inadequate, given

²³⁰ Sartor (n 180) 175.

²³¹ Sartor (n 180) 175.

²³² Marta Maroni and Elda Brogi, 'Freedom of Expression and the Rule of Law: The Debate in the Context of Online Platform Regulation' in Pier Luigi Parcu and Elda Brogi (eds), *Research Handbook on EU Media Law and Policy* (Edward Elgar Publishing 2022) 183.

²³³ Maroni and Brogi (n 232) 184.

²³⁴ Hoboken and others (n 193) 41.

²³⁵ Hoboken and others (n 193) 2. Frosio and Geiger (n 180) 34. Maroni and Brogi (n 232) 184.

²³⁶ Christopher Zara, 'The Most Important Law in Tech Has a Problem' [2017] *Wired* <<https://www.wired.com/2017/01/the-most-important-law-in-tech-has-a-problem/>> accessed 7 January 2025. Maroni and Brogi (n 232) 166.

that they were adopted at a period when digital platforms did not truly exist.²³⁷ Indeed, legislators initially intended to create a harmonized legal framework for Internet Services Providers (ISPs), whose primary functions were to provide internet access or host websites, with only limited intervention on information transmission.²³⁸ Conversely, these rules were not originally designed for Online Services Providers (OSPs),²³⁹ a category that now includes search engines (which were still in their infancy in 2000) and social media platforms (Facebook, for instance, has been publicly accessible only since 2006). In sum, safe harbour rules were conceived for the era of the open web, but the structure of the Internet has changed dramatically over the past decades with the emergence of the so-called platform economy.²⁴⁰ As a result, some scholars argue that these rules are no longer appropriate for regulating the power of large platforms and their extensive content curation practices,²⁴¹ approaching them more similar to media companies. Indeed, while intermediaries, such as telephone companies, are not expected to intervene in message transmission, since they are often unaware of the content being transmitted, content organization is the core service platforms provide,²⁴² rather than simply delivering third-party messages.

The publisher/intermediary dichotomy is also reflected in how platforms portray themselves. In the United States, this debate has been particularly lively, since platforms have sought First Amendment protection by asserting that their content curation activities constitute an autonomous right of expression.²⁴³ In 2024, in

²³⁷ Hoboken and others (n 193) 10.

²³⁸ This does not mean that ISPs cannot intervene on content transmission, even if it's rare. For instance, see Cloudflare case in Nicolas P Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (Cambridge University Press 2019) 8 <<https://www.cambridge.org/core/books/lawless/8504E4EC8A74E539D701A04D3EE8D8DE>> accessed 13 November 2024.

²³⁹ Hoboken and others (n 193) 10.

²⁴⁰ See *supra*: Chapter I, Section 1.

²⁴¹ Bertolini, Episcopo and Cherciu (n 175) III.

²⁴² See *supra*: Chapter I, Section 2.1.

²⁴³ This was the position of a Google advocate in order to defend the platform from accuses of self-favouring: Noam Cohen, 'Professor Makes the Case That Google Is a Publisher' *The New York*

Moody v. Netchoice,²⁴⁴ the Supreme Court of the United States have indeed confirmed such interpretation, stating that:

Like the editors, cable operators, and parade organizers this Court has previously considered, the major social-media platforms curate their feeds by combining “multifarious voices” to create a distinctive expressive offering [...] Their choices about which messages are appropriate give the feed a particular expressive quality and “constitute the exercise” of protected “editorial control.” [...]

Interestingly, the *Netchoice* ruling originated from a Florida law that sought to restrict content moderation activities of major platforms, particularly by limiting their possibility to ‘deplatform’ political candidates and suppress or shadow-ban their posts, while also requiring them to provide an explanation when restricting content.²⁴⁵ The law was introduced in response to conservative concerns that moderation policies disproportionately silenced their views,²⁴⁶ particularly following the removal of Donald Trump’s account on major social media.²⁴⁷ It could be seen as a form of non-discrimination or common carrier regulation, akin to those governing other communication technologies.²⁴⁸ Although the US Supreme Court did not rule on the merits of the law, remanding the case to lower courts and leaving room for future regulation,²⁴⁹ it did affirm that platforms’ content curation practices constitute a form of ‘speech’ protected under the First Amendment. By framing online content curation as a form of expression, the Court recognised that

Times (21 May 2012) <<https://www.nytimes.com/2012/05/21/business/media/eugene-volokh-ucla-professor-makes-a-case-for-google-as-publisher.html>> accessed 19 March 2025. This article refers to: Eugene Volokh and Donald Falk, ‘First Amendment Protection for Search Engine Search Results -- White Paper Commissioned by Google’ (Social Science Research Network, 20 April 2012) <<https://papers.ssrn.com/abstract=2055364>> accessed 19 March 2025.

²⁴⁴ *Moody v Netchoice* [2024] Supreme Court of the United States 22-277.

²⁴⁵ US Congress, ‘Moody v. NetChoice, LLC: The Supreme Court Addresses Facial Challenges to State Social Media Laws’ <<https://www.congress.gov/crs-product/LSB11224>> accessed 9 October 2025.

²⁴⁶ Jack M Balkin, ‘Moody v. NetChoice - The Supreme Court Meets the Free Speech Triangle’ [2025] Yale Law School, Public Law Research Paper <<https://papers.ssrn.com/abstract=5104013>> accessed 8 October 2025.

²⁴⁷ See *supra*: Chapter I, Section 2.1.

²⁴⁸ See *supra*: Chapter I, Section 2.2.

²⁴⁹ Balkin (n 246).

platforms exercise their editorial role through moderation and algorithmic systems. This perspective positions platforms as *speakers* rather than *governors*,²⁵⁰ private entities entitled to express themselves, rather than para-public actors regulating the speech of others. However, when considered alongside Section 230 CDA, the dual protection offered by both free speech rights and safe harbour provisions raises concerns about legal coherence: it creates a framework in which platforms enjoy rights without corresponding responsibilities, fuelling concerns that they are simply benefiting from the best of both worlds.²⁵¹

In addition to this, the exponential rise of fake news, extremist content, and hate speech online in recent years²⁵² has intensified demands for platforms to take stronger action against harmful content and to be held liable if they fail to do so. According to some scholars, safe harbour regulations, following a libertarian approach, inherently facilitate the dissemination of illegal and abusive material online.²⁵³ For the same reason, safe harbour provisions have been criticized for disproportionately harming marginalized groups and minorities, as they enable large communities of misogynists and racists to spread their narratives, reinforcing existing inequalities and injustices in society.²⁵⁴

Requests for broader platform responsibility have been further amplified by cases in which platforms were found to play a direct role in the spread of harmful content due to the design of their algorithms. This phenomenon is generally attributed to the fact that recommender algorithms are designed to maximise user engagement

²⁵⁰ Balkin (n 246).

²⁵¹ Rebecca Tushnet, 'Power Without Responsibility: Intermediaries and the First Amendment' (2008) 76 *George Washington Law Review* 101, 1009 <<https://papers.ssrn.com/abstract=1205674>> accessed 21 November 2024.

²⁵² Bradford (n 2) Introduction. The concerns related to disinformation campaigns after the Brexit referendum and Donald Trump's 2016 election have been already mentioned in Chapter I, Section 2.2 (see: Tambini (n 7) 2.).

²⁵³ Suzor (n 238) 47.

²⁵⁴ Suzor (n 238) 47.

and profit, in line with the logic of the attention economy.²⁵⁵ For instance, YouTube was accused of contributing to terrorist radicalisation by suggesting extremist videos, including ISIS content, to users with related search histories.²⁵⁶ Similarly, Facebook was accused of fuelling hatred against the Rohingya people in Myanmar, thereby contributing to the atrocities and ethnic cleansing campaigns in 2017.²⁵⁷ These concerns were brought before the Supreme Court of the United States in *Gonzalez v. Google* and *Twitter v. Taamneh*,²⁵⁸ which was required to examine whether certain major platforms could be held liable for complicity in terrorist attacks due to their role in recommending ISIS-related content that allegedly facilitated international recruitment. However, the Court ultimately found that, based on terrorism law, platforms' actions did not amount to direct complicity in specific terrorist attacks. As a result, it did not rule on the scope of Section 230 of the CDA and, specifically, on whether its liability shield also extends to content recommendation practices.

To sum up, in an online landscape dominated by large platforms, three factors have contributed to questioning safe harbour regimes:

1. Platforms heavily intervene on information transmission;
2. Illegal content online has become a major political issue;
3. Platforms' algorithms have been found to prioritize harmful content.

Demands for greater accountability for online platforms have gained traction across both civil society and public authorities. The following paragraph will outline key

²⁵⁵ See also: Chapter I; Section 2.1; and Chapter IV.

²⁵⁶ These accusations have been the subject of empirical academic research. See for instance: Murthy (n 134).

²⁵⁷ Amnesty International, 'Myanmar: The Social Atrocity: Meta and the Right to Remedy for the Rohingya' (Amnesty International 2022) <<https://www.amnesty.org/en/documents/asa16/5933/2022/en/>> accessed 19 March 2025.

²⁵⁸ *Twitter, Inc v Taamneh* [2023] Supreme Court of the United States 21–1496; *Gonzalez v Google LLC* [2023] Supreme Court of the United States 21–1333.

changes driven by these demands within the EU, including legislative reforms, policy initiatives, and self-regulatory measures.

1.3. TOWARDS AN ENHANCED RESPONSIBILITY OF ONLINE PLATFORMS WITHIN THE EU

The previous section analysed how safe harbour regimes, shielding online platforms from liability for user-generated content, have increasingly been called into question as the digital landscape has evolved. This situation has prompted European political authorities to reconsider the set of responsibilities established by the ECD. A paramount example of this shifting approach is the European Commission's 2017 *Communication on Tackling Illegal Content Online – Towards an enhanced responsibility of online platforms*.²⁵⁹ Its goal was to urge platforms to combat illegal content, emphasising their 'societal responsibility' to ensure a safer online environment. Even though the underlying intention was not necessarily to amend the regulatory framework established by the ECD, it was acknowledged that platforms must embrace active duties against illegal activities. More specifically, they should recognize their 'central role in society' and act accordingly. This not only requires cooperation with public authorities in reporting illegal activities but also proactive measures to detect and remove illegal content.²⁶⁰

This document was conceived as form of soft law or moral suasion, aiming to encourage the establishment of industry standards. Self-regulation has been indeed facilitated by the adoption of code of conducts by major platforms under the guidance of the European Commission. In 2016, the European Commission reached an agreement with Facebook, Microsoft, Twitter and YouTube on a *Code of*

²⁵⁹ European Commission, 'Communication 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/2017/0555 Final' <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017DC0555>> accessed 7 October 2025.

²⁶⁰ European Commission, 'Communication 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/2017/0555 Final' (n 259).

conduct on Countering Illegal Hate Speech, which other platforms later joined.²⁶¹ The 2018 *Code of Practice on Disinformation*, revised and strengthened in 2022,²⁶² then saw key players agree on standards to combat disinformation. The signatories include major platforms as Google, Meta, TikTok and Twitch,²⁶³ although the platform X have since withdrawn.²⁶⁴ These codes, which initially represented voluntary commitments, were a first step toward greater accountability and then gained new significance under the Digital Services Act, as further discussed below.²⁶⁵

Moreover, in certain sectors, this cultural shift has led to the imposition of binding legal obligations on platforms regarding content moderation. A first example is the EU Directive on Audiovisual Media Services (AVMSD), adopted in 2010 and revised in 2018,²⁶⁶ which marked a significant step toward enhancing responsibility

²⁶¹ See the following website: European Commission, ‘The EU Code of Conduct on Countering Illegal Hate Speech Online’ <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en> accessed 7 October 2025. ‘*In the course of 2018, Instagram, Snapchat and Dailymotion took part to the Code of Conduct, Jeuxvideo.com in January 2019, TikTok in 2020 and LinkedIn in 2021. In May and June 2022, respectively, Rakuten Viber and Twitch announced their participation to the Code of Conduct*’.

²⁶² The Strengthened Code of Practice on Disinformation 2022 is accessible at the following webpage: European Commission, ‘2022 Strengthened Code of Practice on Disinformation | Shaping Europe’s Digital Future’ (*European Commission*) <<https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>> accessed 7 October 2025.

²⁶³ The comprehensive list is accessible at the following webpage: European Commission, ‘Signatories of the 2022 Strengthened Code of Practice on Disinformation | Shaping Europe’s Digital Future’ (*Digital Strategy | European Commission*) <<https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation>> accessed 8 October 2025.

²⁶⁴ Francesca Gillet, ‘Twitter Pulls out of Voluntary EU Disinformation Code’ (27 May 2023) <<https://www.bbc.com/news/world-europe-65733969>> accessed 4 March 2025.

²⁶⁵ See *infra*, Section 2.4.

²⁶⁶ 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), then amended by the Directive 2018/1808 of the European Parliament and of the Council of 14 November 2018.

for harmful content and was widely welcomed.²⁶⁷ It introduced a series of provisions specifically targeting Video-Sharing Platform Services (VSPs), establishing duties of care to protect minors and combat terrorism, incitement to violence, and hatred against groups or individuals.²⁶⁸ However, by not imposing *ex ante* control over information, these provisions have been considered consistent with the prohibition of general monitor obligation established in the Article 15 of the ECD.

Intellectual property rights are another area where enhanced control obligations have been imposed on platforms. The Directive on Copyright established a specific liability mechanism for IP rights infringements, applying to online content-sharing service providers.²⁶⁹ Article 17 of this directive requires platforms to obtain permission from rightsholders (e.g., through licensing agreement) to make protected content uploaded by their users available. In the absence of explicit authorisation, platforms will be held liable, unless they can demonstrate to have undertaken their best efforts to prevent unauthorised content from appearing on their websites.²⁷⁰ The regulation also includes a series of safeguards: platforms are required to minimise the risks of systematic filtering and over-blocking and to provide complaint mechanisms for users contesting content removals.

Finally, additional content moderation obligations have been imposed on hosting providers in the domain of terrorism, specifically through the adoption of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content

²⁶⁷ Bertolini, Episcopo and Cherciu (n 175) 36.

²⁶⁸ AVMSD, Article 28b.

²⁶⁹ 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

²⁷⁰ Bertolini, Episcopo and Cherciu (n 175) 41. This author considers this regulation as instituting a form of primary liability, as host providers are treated as speakers. It is interesting to note that Copyright represents an exceptional domain also in the U.S. legal system, with notice-and-take-down mechanisms.

online.²⁷¹ This regulation requires hosting intermediaries to implement specific measures against terrorism-related content and mandates cooperation with national authorities in this sector. Failure to comply can result in penalties.

None of these regulations have abolished the liability exemption for third-party content established by the ECD, which remains valid as a principle. However, additional duties of care introduced through sector-specific legislation have been said to contribute to its gradual erosion.²⁷² Indeed, cases where platforms are legally required to act against illegal content have increased. In this context, during the development of the EU Digital Single Market Strategy discussions on the adequacy of the ECD liability regime naturally emerged.²⁷³ Despite concerns about platforms' role in content curation, the safe harbour principle was still considered essential to safeguarding online freedom. Consequently, the final decision was to reintroduce the conditional exemption system in the new Digital Services Act ('DSA').²⁷⁴ Although Articles 12, 13, 14 and 15 of the ECD have been repealed and replaced by the new DSA provisions, the core principles of intermediary liability remain unchanged. However, the scope of the liability exemption has been significantly narrowed due to the introduction of a series of general duties to act with respect to illegal content. The following section will present the new rules structuring the liability regime for platforms under the DSA.

2. THE LIABILITY REGIME FOR ONLINE PLATFORMS AND MANDATORY MODERATION ACTIVITIES UNDER THE DSA

The DSA fully entered into force for all intermediaries on February 17, 2024. However, it had already been applied since the end of August 2023 for rules

²⁷¹ Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

²⁷² Bertolini, Episcopo and Cherciu (n 175) 29. Maroni and Brogi (n 232) 186.

²⁷³ Communication from the Commission, *A Digital Single Market Strategy for Europe*, par. 3.3 (COM/2015/0192/ final).

²⁷⁴ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Online Platforms and the Digital Single Market Opportunities and Challenges for Europe*, COM/2016/0288 final.

targeting Very Large Online Platforms, as previously identified by the European Commission.²⁷⁵ This means that some of its provisions may be commented in the light of their practical application.

According to the European Commission, the main goal of the Digital Services Act is to prevent illegal and harmful activities online and combat the spread of disinformation, while ensuring user safety, protecting fundamental rights, and promoting a fair and open platform environment.²⁷⁶ Simultaneously, it aims to provide legal certainty, foster innovation, and support the growth of SMEs and start-ups in digital markets. Notably, whereas the second set of objectives was already broadly pursued under the previous regulatory framework, the ECD, the first set underlines the new approach pursued by the DSA, i.e. the alignment of the current digital landscape with European values.

Following the political agreement between the European Parliament and the Council on the adoption of the DSA, EU Commissioners highlighted the increased accountability required from the largest online platforms. Margrethe Vestager, former Executive Vice-President for a Europe Fit for the Digital Age, stated: *‘With today's agreement we ensure that platforms are held accountable for the risks their services can pose to society and citizens’*; while Thierry Breton, former Commissioner for the Internal Market, added: *‘With the DSA, the time of big online*

²⁷⁵ As defined in the following paragraph.

²⁷⁶ See the following webpage: European Commission, ‘The EU’s Digital Services Act’ (*European Commission*, 27 October 2022) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en> accessed 7 October 2025. This also emerges from the preamble of the DSA, namely Recital (9) states that the objective of the regulation is creating a safe online environment, where fundamental rights are protected, innovation is fostered, all in countering the spread of illegal and harmful content. See also: European Commission, ‘Commission Staff Working Document | Impact Assessment Accompanying the Document | 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 | SWD/2020/348 Final’ <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020SC0348>> accessed 7 October 2025.

*platforms behaving like they are ‘too big to care’ is coming to an end’.*²⁷⁷ The scope and characteristic of this new accountability will be analysed in the following pages.

The liability of intermediary services is regulated by the first part of the DSA. It essentially mirrors the ECD, with the same conditions for exemption applying to mere conduit (Article 4 of the DSA), caching (Article 5) and hosting (Article 6).²⁷⁸ The prohibition of imposing general monitoring obligations, previously contained in Article 15 of the ECD, is also transposed in the DSA, under Article 8. However, it must be noted that the DSA rules out the issue of defining ‘*passivity*’, since the preamble of the Regulation no longer includes this requirement.²⁷⁹ Furthermore, the recital that specifies that the provider must not be in any way involved with users’ content now applies only to mere conduit and caching services, suggesting that hosting providers may, to a certain extent, engage with such content.²⁸⁰ Similarly to the ECD, the Regulation only harmonises cases of immunity, while liability regimes continue to follow national rules, posing significant risks of fragmentation among different Member States.²⁸¹

The principle of conditional exemption is thus maintained under the new framework. Focusing on hosting providers, the DSA reaffirms that they are not liable for third-party content unless they become aware of its illegality, either spontaneously or through notification, and fail to act to remove it. However, there are several innovations broadly affecting the liability regime. First, the DSA

²⁷⁷ European Commission, ‘Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment’ <https://ec.europa.eu/commission/presscorner/detail/en/https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545> accessed 4 March 2025.

²⁷⁸ Wilman (n 204) 38.

²⁷⁹ DSA, Recital 28: ‘The exemptions from liability established in this Regulation 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’.

²⁸⁰ Wilman (n 204) 41. Reference is to DSA, Recital 22.

²⁸¹ Aina Turillazzi and others, ‘The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications’ <<https://papers.ssrn.com/abstract=4007389>> accessed 13 November 2024.

introduces an explicit Good Samaritan Protection for intermediaries engaging in voluntary content moderation activities, but coupled with a duty to report certain types of illegal activities eventually encountered (Section 2.2). Second, several provisions modify the obligations borne by intermediaries when dealing with illegal content. Notably, as notifications submitted by public authorities and users are now regulated at the EU level, the notion of ‘*awareness*’ of illegality is further specified (Section 2.3). Moreover, for platforms classified as VLOPs or VLOSEs, additional due diligence obligations towards illegal and harmful content are introduced (Section 2.4).

However, these rules do not apply to all intermediaries but only to selected categories. For this reason, before illustrating the new rules affecting liability, it is necessary to preliminarily describe the scope of application of the DSA, which follows a peculiar structure of escalating obligations based on the characteristics and dimensions of the intermediary at stake (Section 2.1).

2.1. SCOPE OF THE DSA: THE ESCALATING OBLIGATIONS SYSTEM

Contrary to the Electronic Commerce Directive, the Digital Services Act exclusively applies to information service providers acting as intermediaries.²⁸² In this sense, it may be seen as an expansion of Section 4 of the ECD, which is the only part of the Directive to be simultaneously repealed.²⁸³

The DSA follows a peculiar structure of escalating obligations based on the characteristics and dimensions of the intermediary. The complexity of the new regulation reflects the intricacies of the digital landscape 20 years after the adoption of the ECD. This is also evident from the considerable difference in length between the two regulations: while the ECD consists of only 15 pages, 24 articles, and 65 recitals, the DSA spans 102 pages, 93 articles, and 156 recitals. This expansion

²⁸² The scope of the ECD has been described above: Section 1.1.

²⁸³ DSA, Article 89(1): ‘Articles 12 to 15 of Directive 2000/31/EC are deleted’.

contributes to greater clarity in several provisions, which are now more detailed, although some questions remain open.

The structure of escalating obligations implies that the DSA identifies multiple types of intermediaries, each subject to partially different rules. Building on the distinction among mere conduit, caching and hosting intermediaries established by the ECD, it introduces additional classifications within the category of hosting intermediaries. As a result, the first category bearing additional obligations consists of hosting providers, which, among the three categories originally addressed by the ECD, have undergone the most significant transformation.²⁸⁴

Secondly, the DSA imposes further duties on online platforms, a subcategory of hosting providers whose main function is to disseminate information to the public.²⁸⁵ Like traditional hosting providers, online platforms' activity consists in storing and eventually distributing information at the request of individual users. The main difference is that platforms also able to publicly disseminate the information at the request of the recipient. The concept of *public dissemination* is clarified by the preamble of the DSA: it is understood as making information available to a potentially unlimited number of persons, thereby making it accessible to all recipients of the service.²⁸⁶ In principle, accessing the information should not require further action from the recipient. However, if accessing the information requires, for instance, registration to a group, the information is still deemed public when the access is automatic and does not involve human intervention. Conversely, private messaging services fall outside this definition, except for public groups or open channels.²⁸⁷ The preamble also specifies that the qualification of platform

²⁸⁴ See *supra*: Section 1.2.

²⁸⁵ DSA, Article 1(i). See also: Chapter I.

²⁸⁶ DSA, Recital 13.

²⁸⁷ DSA, Recital 14.

should not apply if the public dissemination constitutes merely a minor service provided (e.g., a comment section in an online newspaper or cloud computing).

The third category bearing additional obligations in the DSA encompasses online platforms that enable consumers to conclude distance contracts with traders, i.e. online marketplaces. Section 4 of the DSA is specifically dedicated to this category and include some additional rules, which are not however analysed in the context of this research, as it mainly focuses on the transmission of non-commercial information.

Finally, the last category covers Very Large Online Platforms and Very Large Online Search Engines (hereafter referred to as ‘VLOPs’ and ‘VLOSEs’ for simplicity). This classification follows a dimensional criterion based on the number of average monthly active users, which must, in principle, be equal or exceed 45 million.²⁸⁸ The identification of this category is particularly relevant to the purposes of this research, which focuses on the impact of major platforms on information flows. Alongside the ‘gatekeeper’ definition in the DMA,²⁸⁹ it represents the first legal definition of what is commonly referred to, in the socio-economic debate, as GAFAM, Big Tech, or Web/Tech/Digital Giants. The European institutions have acknowledged that this kind of platforms play a major role in facilitating public debate (as well as in economic operations) and in shaping the way information, opinions and ideas circulate.²⁹⁰ Their crucial role in information flows represents a public policy concern and, therefore, justifies and demands the imposition of specific obligations. Indeed, their position is linked to the need to address ‘systemic

²⁸⁸ DSA, Article 33(1). It represents the 10% of the EU population. According to the provisions contained in the same article, the number may be changed by the Commission based on the possible increase or decrease of Union’s population.

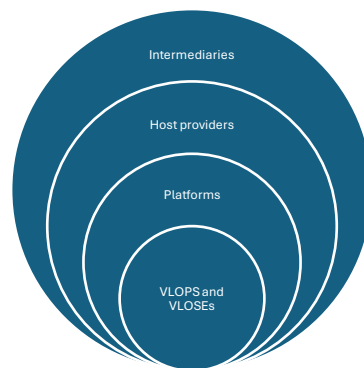
²⁸⁹ See *infra*, Chapter IV, Section 2.1.

²⁹⁰ DSA, Recital 75.

risks’ possibly associated to the use and functioning of their services, which require an adequate response.²⁹¹

For greater clarity, the following figure (Figure 1) illustrates the hierarchical structure of intermediaries under the DSA, following the principle of escalating obligations. Only the categories most relevant to this research have been selected.²⁹² The ‘intermediary’ category represents the broadest definition. Certain intermediaries may then qualify as hosting providers, some hosting providers may also fall within the definition of online platforms, and some platforms may be designated by the EU Commission as VLOPs or VLOSEs. As a result, VLOPs and VLOSEs are subject to all the obligations applying to online platforms, hosting providers and intermediaries, and to some additional specific requirements.

Figure 1. Main categories of information society services addressed by the DSA following the structure of escalating obligations.



Having outlined the types of online intermediaries covered by the DSA, the remainder of this section focuses on the main innovations affecting their liability regimes and their obligations concerning the dissemination of illegal content.

2.2. THE GOOD SAMARITAN PROTECTION AND REPORTING OBLIGATIONS

²⁹¹ DSA, Recital 79. See *infra*: Section 2.4.

²⁹² Caching and mere conduit services, as well as online marketplaces, although addressed by the DSA, are not represented in the figure.

The first innovation introduced by the DSA concerns the establishment of an explicit Good Samaritan Protection. Article 7 of the DSA states that the liability exemptions are not affected by the fact that the intermediary service carries out voluntary investigations or takes other measures to identify and disabling access to illegal content. Although this principle was already considered applicable in the EU legal order,²⁹³ its explicit recognition enhances legal certainty and conclusively excludes the possibility that the intermediary nature of the service is affected by voluntary content curation practices addressing illegal content. However, Article 7 introduces the additional conditions of ‘good faith’ and ‘diligence’, which are effectively new in the EU context. As open-ended standards, their precise content remains to be clarified, but, according to some authors, they are likely to be interpreted in light of the broader diligence obligations set out elsewhere in the Regulation.²⁹⁴

The principle established by Article 7 is comparable to the second part of Section 230 of the Communications Decency Act in the U.S. (the ‘Good Samaritan’). The goal is the same, namely not to discourage providers from spontaneously acting against illegal content, while safeguarding the liability exemption mechanism with the purpose of mitigating over-removal risks to the detriment of freedom of expression.²⁹⁵ However, it is noteworthy that Article 7 of the DSA only mentions actions against ‘illegal’ content and not against any ‘objectionable’ content, as envisaged by Section 230. This potentially leaves open the question of how to qualify the removal of content that is not illegal but merely against the terms and conditions of the service.²⁹⁶

As mentioned before, the resulting system is coherent but somewhat fictional, considering the extent to which platforms engage in content curation, thereby seriously undermining the concept of neutrality and, more specifically, the notions

²⁹³ See *supra*, Section 1.

²⁹⁴ Wilman (n 204) 45.

²⁹⁵ Bertolini, Episcopo and Cherciu (n 175) IX.

²⁹⁶ This question is further developed below, in Chapter 0, Section 1.

of lack of knowledge and control, which are supposed to represent the rationale of the whole safe harbour regulation.²⁹⁷ In this context, it is worth noting that Article 18 introduces a reporting obligation for intermediaries qualifying as hosting provider in relation to certain illegal activities. More precisely, under this provision, hosting services, including platforms, are obliged to notify national authorities upon becoming aware of any information raising suspicion of serious criminal offences. The possibility for Member States to impose such obligations was already envisaged by the ECD,²⁹⁸ but the DSA has created a harmonised obligation to this regard within the European Union. Specifically, this obligation concerns very serious criminal offences, which involve a threat to the life or safety of a person that has already occurred, is occurring, or is likely to occur.²⁹⁹

This provision, despite enhancing intermediaries' obligations regarding illegal content, does not alter their liability regime. Non-compliance with this obligation may only result in the application of penalties following Article 52. However, in line with Article 6, if the information is illegal, intermediaries must promptly remove it to maintain their liability exemption. Moreover, it is important to note that this provision does not impose any additional monitoring obligations on providers, as the obligation to notify authorities only arises if the intermediary becomes aware of the information accidentally, for instance in the context of voluntary monitoring activities. Overall, this reporting obligation has the merit to connect the right to monitor and moderate user content to some form of societal responsibility.

2.3. 'AWARENESS' OF ILLEGALITY AND NOTICE-AND-ACTION MECHANISMS

²⁹⁷ See *supra*: Section 1.1.

²⁹⁸ ECD, Article 15(2).

²⁹⁹ The notification must be directed to the enforcement or judicial authorities of the Member States where the offence may be situated or, if the location cannot be identified, where the provider is established.

As already mentioned, hosting providers benefit from a liability exemption for third-party content, unless they are aware of its illegality and fail to remove it.³⁰⁰ Therefore, liability exemptions for hosting providers hinge on the notions of lack of knowledge and awareness regarding illegal content, as well as prompt action once such knowledge is acquired. Importantly, certain provisions of the DSA help defining the conditions under which such awareness can exist, thereby narrowing the scope of the immunities. These provisions include those regulating injunctions from national authorities, as well as those regulating notifications submitted by users.

Injunctions from national authorities can be issued to compel an intermediary provider to remove illegal content or to obtain information about user activities. Although their impact on liability is not explicitly addressed by the Regulation, they are closely connected to it, because of their capacity to trigger awareness. These measures are regulated by Article 9 and 10 of the DSA and will be analysed in the first subsection. Next, the DSA requires hosting providers to enable users to trigger notice-and-action mechanisms for reporting illegal content. In this regard, Article 16 of the DSA explicitly mentions the possibility of liability for failure to remove the reported illegal content. This provision is analysed in the second subsection, together with the rules concerning the establishment of a trusted-flaggers system. Finally, when analysing platforms' duties to act in relation to illegal content, it is worth mentioning the obligation for online platforms to impose restrictions on users in the case of abusive conduct, as illustrated in third subsection.

Injunctions and information requests by national authorities

As previously mentioned, the ECD, while preventing Member States from imposing general monitoring obligations on intermediary providers, allowed them to issue specific orders to act against illegal content, in line with their national

³⁰⁰ DSA, Article 6 (1).

rules.³⁰¹ The DSA goes further on this point, by harmonising the minimum conditions that injunctions and information requests transmitted by national authorities to intermediary providers must meet in order to produce an obligation to act under EU law. Indeed, Article 9 outlines the procedure for transmitting a takedown order and specifies the information it must contain. The order must include sufficient information to enable the precise identification of illegal content and the reasons justifying the request. If the order complies with these requirements, the addressee will be obliged to inform the competent authorities of the action taken in this regard without undue delay. A similar mechanism is established regarding the issuance of orders to provide information by national authorities, the requirements for such a request to imply an obligation to respond being detailed in subsequent Article 10. These orders are issued, for instance, when the provider holds information necessary to identify the author of an online illegal activity.

It should be noted that, in both cases, the obligation incumbent on the intermediary is not to act in compliance with the order (i.e., remove the content or provide the information), but to communicate as soon as possible the action taken in this regard. For this reason, the mechanism established by these articles should be regarded as a ‘notice-and-action’ mechanism, rather than a ‘note-and-take-down’ one. It appears therefore legitimate for the addressee not to comply with the order, as long the reasons for such conduct are adequately explained.

Closely related to the prescriptive character of the orders under Articles 9 and 10 is the question of awareness of illegality, and its connection with liability exemptions. Despite the adoption of common rules, the DSA does not clarify whether the transmission of an order that complies with its rules automatically entails awareness of illegality on the part of the intermediary. To understand the impact of such

³⁰¹ ECD, Recital 47.

notifications on the awareness of illegality, it is useful to reference to the case-law of the Court of Justice based on the ECD framework.

In the *L'Oréal* case,³⁰² the CJEU ruled on the link between the notification of a takedown order and the awareness of the illegality of the content at stake. It emphasised that a takedown order for illegal content addressed to a hosting provider may lead to the latter being deemed aware of the illegality in question, resulting in a loss of immunity under Article 14 ECD. However, this case-law does not acknowledge any automatic correlation between a removal order and the awareness of illegality, which must be assessed by the national court on a case-by-case basis.³⁰³ In this regard, the Court stated:

'[...] although such a notification admittedly cannot automatically preclude the exemption from liability provided for in Article 14 of Directive 2000/31, given that notifications of allegedly illegal activities or information may turn out to be insufficiently precise or inadequately substantiated, the fact remains that such notification represents, as a general rule, a factor of which the national court must take account when determining, in the light of the information so transmitted to the operator, whether the latter was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality'.³⁰⁴

It follows that, under the ECD, the loss of immunity following a takedown order depends on the characteristics of the removal order and, in particular, on whether it is sufficiently precise and reasoned.

The principle stated by the Court of Justice in the *L'Oréal* case could guide the determination of the impact of an order transmitted in line with Article 9 and 10 of the DSA on the intermediary's awareness and, consequently, on the liability exemption. Considering that the Court held that the awareness of the illegality must be assessed based on the precision and reasoning of the order, and given that Article 9 and 10 of the DSA aim to define these requirements for an order to be effective,

³⁰² CJEU, *L'Oréal* (n 208).

³⁰³ *Hoboken and others* (n 193) 39.

³⁰⁴ CJEU, *L'Oréal* (n 208), §122.

it seems reasonable to assume that the transmission of an order that complies with these articles generally implies the awareness of illegality, resulting in the loss of immunity. This interpretation appears even more plausible in light of the provisions of Article 16 of the DSA, analysed in the following subsection.

Reporting mechanisms accessible by users and trusted flaggers

A completely new provision introduced by the DSA concerns the regulation of notice-and-action mechanisms accessible to users. Article 16 of the DSA requires hosting providers to establish a system allowing users to report illegal content.³⁰⁵ While reporting mechanisms accessible to users were already present on major platforms, the novelty of this provision relies in the fact that these mechanisms now trigger a right to a decision and, potentially, result in the provider being held liable for failing to remove the flagged content. Indeed, under Article 16, hosting providers must, without undue delay notify the person or entity who submitted the notice of the decision taken regarding the flagged content, and indicate available avenues for redress.³⁰⁶ As with injunctions, the provider's obligation upon receiving a notice is not to automatically remove or restrict the content, but rather to assess the notice and take appropriate follow-up measures. Notably, the provider's decision does not need to be accompanied by a statement of reason, unlike what Article 17 establishes for content restriction decisions.³⁰⁷ Conversely, the redress mechanisms established by the DSA for content restrictions (namely, internal complaint handling systems and out-of-court dispute settlement bodies) also apply to the notice-and-action procedure.³⁰⁸

³⁰⁵ It is noteworthy that while Article 9 and 10 are applicable to all intermediary providers, Article 16 only applies to hosting providers, in line with the escalating obligations structure.

³⁰⁶ DSA, Article 16(5).

³⁰⁷ Ortolani (n 20) 156. On Article 17, see *infra*: Chapter 0, Section 1.2.

³⁰⁸ Those are internal complaints mechanisms (Article 20) and out-of-court dispute settlement bodies (Article 21). See *infra*: Chapter III, Section 1.2.

Importantly, Article 16 only refers to the possibility for users to report illegal content. However, as largely discussed above,³⁰⁹ certain categories of non-illegal content are nevertheless incompatible with platforms' terms and conditions. This can include certain categories of hate speech and false information. For these types of harmful content, the availability of a notice mechanism depends on the platforms, which remain free to determine the purview of user affordances.³¹⁰

Article 16 also explicitly establishes that, whenever a notice submitted by one user is sufficiently precise, the provider is deemed to acquire awareness about the reported illegality, thereby opening the way for liability in line with Article 6(1).³¹¹ Accordingly, a notice is considered sufficiently precise when it enables a diligent provider to identify the illegality without requiring a detailed legal examination. In this case, contrary to what was discussed in the previous subsection regarding injunctions, the link between notification and liability is positively established by the DSA. However, similarly to what has been established in *L'Oréal* in that context, the connection is not automatic and depends on the notification being sufficiently precise and not requiring a detailed legal examination on the part of the hosting provider. This means that, also in this context, a judicial examination on a case-by-case basis assessing whether the user notification possess the requirements to trigger awareness is required. On this point it is worth noting that Article 44 of the DSA promotes the standardisation of the electronic submission of Article 16 notices.³¹²

As mentioned above, treating notifications issued by national authorities differently from those submitted by users in terms of their impact on liability exemptions lacks logical coherence. In fact, if user notifications can trigger awareness and liability,

³⁰⁹ See *supra*: Chapter I, Section 2.1. This issue is also further discussed below, in the introduction of Chapter III.

³¹⁰ Ortolani (n 20) 156.

³¹¹ DSA, Article 16(3).

³¹² Ortolani (n 20) 156.

an injunction issued by national authorities should do so *a fortiori*. As a result, both sets of provisions should be regarded as contributing to the definition of awareness and, consequently, redefining the boundaries of liability exemptions. Nonetheless, one difference between Article 16 and the *L'Oréal* principle is that the former introduces an additional criterion to assess the link between notification and awareness, namely the lack of necessity for a detailed legal examination on the part of the provider. The meaning of this criterion is unclear: it could be interpreted as focusing on the nature of the illegality at stake (i.e., manifest illegality), rather than on the content of users' notifications. Indeed, it remains uncertain whether a notification could be effective in cases where the illegality is not apparent but must be proven or requires a balance between divergent interests (e.g., for defamation). Once again, the interpretation of this criterion will ultimately be determined by national courts or, in the context of preliminary rulings, by the Court of Justice. In any case, this criterion could reasonably be seen as pertaining only to the assessment of user notifications and not to notifications issued by national authorities. In fact, unlike users, national authorities generally possess the competence to determine the illegality of a content, and therefore the provider should, in principle, adhere to the assessment made by the authority.

Reporting mechanisms accessible to users play a crucial role in content moderation, serving as a decentralised and democratic form of control. Also, as harmful content often targets specific users, they are in best position to notify platforms such information. Despite its merits, flagging also presents a series of challenges. In particular, its massive use as harassments technique or by malicious actors and bots may render it unreliable.³¹³ To address these issues, a system of trusted flaggers has been introduced by the DSA for online platforms, aiming at maintaining the benefits

³¹³ Gillespie (n 60) 130.

of users' control while mitigating its drawbacks. By involving users deemed trustworthy, the reliability of the moderation process sees improvement.

This solution is not novel, having already been included in some voluntary programs in the past.³¹⁴ Article 22 of the DSA has the merit to generalise this system for all online platforms, requiring them to take necessary technical and organisational measures to ensure that notices submitted by trusted flaggers are given priority and are decided upon without undue delay. Trusted flaggers status is granted, upon application, by the Digital Services Coordinator of the Member State where the applicant is established.³¹⁵ It is awarded based on the applicant's a specific area of expertise and the applicant must demonstrate that it meets various conditions regarding its experience in identifying illegal content and its independence. While past spontaneous implementations by platforms faced transparency issues as the identity and activity of these flaggers remained undisclosed, the DSA imposes transparency obligations on both platforms and trusted flaggers. In fact, trusted flaggers must annually report their activities, and the Commission maintains a publicly accessible database.

More generally, human rights associations have criticised notice-and-action mechanisms, fearing they may pose a risk of over-removal, particularly when handling individual reports, following the logic 'delete first, think later' to avoid responsibility.³¹⁶ In fact, while liability for failure to remove content is envisaged, there is no corresponding liability for having removed lawful content. Nonetheless, the DSA introduced certain safeguards for moderation procedures, which include

³¹⁴ Gillespie (n 60) 131. Examples include: (a) YouTube trusted flaggers program, introduced in 2012, in the form of a system of rewards based on accuracy of former flagging activities; (b) Twitter partnership with the association Women Action and the Media to help combatting gender harassment.

³¹⁵ A procedure to suspend the status of trusted flagger in case of misbehaviour is also established: DSA, Article 22(6).

³¹⁶ Jan Penfrat, 'The EU's Attempt to Regulate Big Tech: What It Brings and What Is Missing' (*European Digital Rights (EDRi)*, 18 December 2020) <<https://edri.org/our-work/eu-attempt-to-regulate-big-tech/>> accessed 4 March 2025.

the obligation to act diligently and in compliance with human rights.³¹⁷ Moreover, as further discussed below, the obligation for platforms to establish complaint mechanisms, and especially independent out-of-court dispute settlement bodies, may help mitigate this risk.³¹⁸

With regards to trusted-flaggers systems, the idea of prioritising some category of flaggers represent an interesting approach from a perspective of shared governance of online speech. It enables diverse actors, such as specialised police forces and anti-discrimination associations, who act in the public interest or in the interest of specific communities, to participate in content removal. However, over-removal risks may be even higher in this context, as trusted flaggers recognised expertise may lead online platforms to restrict content without in-depth review.³¹⁹ Particular caution should therefore be exercised in the designation of these actors, in order to prevent the emergence of partisan or politically motivated forms of censorship.

Measures against abusive conducts by users

Another provision worth analysing with respects to the new duties of online platforms regarding illegal content is Article 23 of the DSA. This article requires hosting providers qualifying as platforms to adopt measures against abusive conducts carried out by users,³²⁰ meaning that they must suspend services towards users who repeatedly violate the law. Some general criteria to identify such abusive conduct are provided, namely the number of illegal contents provided, the relative

³¹⁷ DSA, Article 14. See *infra*: Chapter III, Section 1.

³¹⁸ Penfrat (n 316).

³¹⁹ Sebastian Felix Schwemer, 'Trusted Notifiers and the Privatization of Online Enforcement' (2019) 35 Computer Law & Security Review 105339, 8 <<https://www.sciencedirect.com/science/article/pii/S0267364918304436>> accessed 9 May 2025. This is in line with the European Commission's Recommendation 2018/334 (rec. 29), stating that every report submitted by trusted flaggers should be treated with 'an appropriate degree of confidence as regards their accuracy' (Jacob Kerkhof (van de), 'Article 22 Digital Services Act: Building Trust with Trusted Flaggers' (2025) 14 Internet Policy Review <<https://policyreview.info/articles/analysis/article-22-digital-services-act>> accessed 11 April 2025.)

³²⁰ DSA, Article 23. The obligations for platforms mentioned in this paragraph only concern moderation activities. The ones concerning advertisement and recommender systems will be examined in the next chapter.

proportion in relation to the total number of information provided, the gravity, and, if identifiable, the intention. Such suspension shall occur for a reasonable period of time, following a prior warning. Moreover, information about these measures must be clearly communicated in terms and conditions of use. This provision implies that the DSA not only *tolerates* moderation conducted through particularly restrictive measures such as account suspension but, in certain cases, *mandates* it. Article 23(2), for its part, deals with a different type of abuse, consisting of frequently submitting notices or complaints that are manifestly unfounded. In this case it is the processing of notice and complaints from that particular recipient that must be suspended.

In addition to these provisions, major platforms designated as VLOPs or VLOSEs, must assess and mitigate the risks of disseminating illegal and harmful content through their services. The relevant provisions are analysed in the following section.

2.4. VLOPs AND VLOSES SPECIAL ACCOUNTABILITY FOR ILLEGAL AND HARMFUL CONTENT

Another part of the DSA where enhanced accountability for illegal content is envisaged concerns the provisions specifically addressed to VLOPs and VLOSEs. As mentioned in Section 2.1, under the system of escalating obligations, these very large platforms and search engines are subject to a dedicated section of the DSA introducing additional duties reflecting their particular role and the public policy concerns it raises. After analysing the definition of VLOPs and VLOSEs, this section turns to the analysis of the specific obligations applying to them that affect the responsibility framework, namely the provisions on systemic risks, on code of conducts and on the introduction of a crisis mechanism.

Designation of VLOPs and VLOSEs by the European Commission

Contrary to other classifications included in the DSA, application of additional obligations for this category of intermediaries is not automatic but follows

designation by the European Commission.³²¹ The European Commission must identify VLOPs and VLOSEs based on the criteria outlined in Article 33 of the DSA, which requires, in principle, a number of average monthly active user in the EU equal to or higher than 45 million (i.e., to 10% of the EU population). To this end, by 17 February 2023, and subsequently every six months, platforms must publish the average number of active users on their services within the European Union.³²²

The first designations were made on 25 April 2023. Initially, VLOPs included several social media platforms (LinkedIn, Facebook, Instagram, Pinterest, Snapchat, TikTok, X), major marketplaces (AliExpress, Amazon, Zalando, Google Shopping), app stores (Google Play, Apple Store), and services such as Booking.com, YouTube, Wikipedia, and Google Maps. The VLOSEs designated were Google Search and Bing. Subsequently, platforms for sharing pornographic videos such as Pornhub, Stripchat, XVideos were designated as VLOPs on 20 December 2023. The marketplaces Shein and Temu followed on 26 April 2024 and 31 May 2024, respectively.³²³ Lastly, WhatsApp has been designated as VLOP in January 2026.³²⁴

The designation of these intermediaries has at times been contested by the companies concerned. For instance, both Amazon and Zalando have challenged their designation decisions bringing an action before the Court of Justice against

³²¹ DSA, Article 33(1) and (4).

³²² DSA, Article 24(2).

³²³ List available here: European Commission, 'Supervision of the Designated Very Large Online Platforms and Search Engines under DSA' (*Shaping Europe's digital future | European Commission*) <<https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>> accessed 21 March 2025.

³²⁴ European Commission, 'Commission Designates WhatsApp as Very Large Online Platform under the Digital Services Act |' <<https://digital-strategy.ec.europa.eu/en/news/commission-designates-whatsapp-very-large-online-platform-under-digital-services-act>> accessed 11 February 2026.

the Commission.³²⁵ Zalando argued that the Commission misunderstood the nature of its services,³²⁶ since their intermediary component represents only a minor portion of Zalando's business model (accounting for 37% of global sales). Moreover, even for this portion, Zalando highlighted that the information uploaded by third parties is consistently checked and modified by the platform. On this point, the General Court interestingly held that the criterion of neutrality is irrelevant for determining whether a service qualifies as an intermediary provider, as this classification depends solely on the carriage of third-party content. The role of neutrality is therefore confined to liability exemptions.³²⁷ Following this interpretation, the CJEU's case-law on passivity³²⁸ is not pertinent to the application of the due diligence obligations established by the DSA.³²⁹ Moreover, Zalando's designation as VLOP in its entirety, regardless of the fact that most of its sales are made directly from Zalando itself, was justified since users navigating the platform are simultaneously exposed to both Zalando's and third-party content.³³⁰

On the other hand, some relevant services are currently absent from the Commission's list of designation, which is likely to expand over time. Personal messaging applications were long excluded, even though some popular services, such as Telegram and WhatsApp, display features comparable to social media platforms, notably open channels and public groups that allow users to broadcast messages to large audiences.³³¹ As previously mentioned, Recital 14 of the DSA

³²⁵ CJEU, Case T-367/23, *Amazon Services Europe v Commission*, action brought on 5 July 2023; and Case T-348/23, *Zalando v Commission*, action brought on 27 June 2023.

³²⁶ Zalando, 'Zalando: Zalando Files Legal Action against the European Commission to Contest Its Designation as a "Very Large Online Platform" as Defined by the Digital Services Act' (*Zalando Corporate*, 27 June 2023) <<https://corporate.zalando.com/en/company/zalando-files-legal-action-against-european-commission-contest-its-designation-very-large>> accessed 21 March 2025.

³²⁷ *Zalando v European Commission* [2025] Court of Justice of the European Union, General Court ECLI:EU:T:2025:821, T-348/23.

³²⁸ As presented in Section 1.2.

³²⁹ CJEU, *Zalando* (n 327), §35-42. See also: DSA, Recital 18.

³³⁰ CJEU, *Zalando* (n 327), §67.

³³¹ Anna Vicinanza, 'La responsabilità delle piattaforme digitali nei confronti dei contenuti illegali: dal caso Telegram al Digital Services Act' [2025] Quaderni AISDUE 195

excludes private messaging services from the definition of online platform, with the exception of open channels and public groups. Indeed, WhatsApp has recently been designated as VLOP, whereas Telegram declared that it has not reached the relevant user threshold. Similarly, Airbnb is not included in the list, despite offering a service structurally comparable to Booking.com, as both facilitate the rental of accommodation by connecting hosts and guests. Spotify also performs an intermediary function by distributing music and podcasts created by third parties to a wide audience. Operating as a platform for content distribution and access, it represents a key player within the audio-streaming market. Yet, both Airbnb and Spotify reportedly did not reach the threshold of 45 million average monthly active users.³³² Conversely, Netflix, who provides a video-streaming service, operates more as a publisher than an intermediary: it does not allow user to upload their content, but directly curates its selection, and therefore is not likely to be designated as VLOP.

Having illustrated the notion of Very Large Online Platform and Very Large Search Engine, the next subsections are dedicated to the description of their main obligations in relation with illegal and harmful content.

Systemic risks assessment and mitigation measures: a new obligation to moderate content?

The first specific obligation regarding VLOPs and VLOSEs is to assess the systemic risks stemming from the design or functioning of their service or the ways these services are used. This risk assessment must be conducted annually and before

<<https://www.aisdue.eu/anna-vicinanza-la-responsabilita-delle-piattaforme-digitali-nei-confronti-dei-contenuti-illegali-dal-caso-telegram-al-digital-services-act/>> accessed 3 March 2025.

³³² Also other popular platforms declared not to reach this threshold (e.g., Reddit, ‘Digital Services Act (DSA): Information for EU Users’ (*Reddit Help*, 15 August 2025) <<https://support.reddithelp.com/hc/en-us/articles/23595536875796-Digital-Services-Act-DSA-Information-for-EU-users>> accessed 27 October 2025.). Company declarations on user thresholds dating from 2023 can be found at: Husovec, Martin, ‘DSA – Monthly Active Users – Second Disclosure’ <<https://husovec.eu/wp-content/uploads/2023/09/DSA-MAU-Second-Disclosure-Aug2023.pdf>>.

introducing any new functionality. The assessment must include an analysis of the following risks: **(a)** the diffusion of illegal content; **(b)** the negative effects on fundamental rights and, especially, human dignity, privacy, freedom of speech and expression (including media freedom and pluralism), non-discrimination and consumers' rights; **(c)** the negative effects of civic debate, electoral process and public security; **(d)** the negative effects on gender-based violence, public health, protection of minors and individual' physical and mental well-being.³³³ In the light of this assessment, VLOPs and VLOSEs must subsequently put in place reasonable, proportionate and effective mitigation measures, bearing in mind fundamental rights' protection.³³⁴ Such measures may include, *inter alia*, adaptation of their terms and conditions and their enforcement; adaptation of content moderation processes; adjustment of cooperation with trusted flaggers and of implementation of the decision of out-of-court dispute settlement bodies; targeted measures to protect minors; and warnings about manipulated audio-visual content.³³⁵ Interestingly, a binding obligation to flag artificially manipulated content and *deepfakes* can be found under the AI Act,³³⁶ which is applicable to digital platforms since they often classify as AI systems deployers.

These provisions on systemic risks assessment for VLOPs and VLOSEs sparked a considerable debate about whether they create additional moderation duties. Importantly, these duties may encompass not only illegal content but also content that is merely *harmful*. This interpretation is connected to the mentioning of disinformation and certain types of violent content, which are not equally illegal across Member States. Moreover, the DSA's preamble explicitly requires

³³³ DSA, Article 34.

³³⁴ DSA, Article 35.

³³⁵ Following risk assessment by major platforms, the European Board for Digital Services ('EBDS'), an independent advisory group of Digital Services Coordinators with functions of supervision on providers of intermediary services, in cooperation with the Commission, must publish a comprehensive report once a year that includes the most prominent and recurrent systemic risks reported, along with the best practices.

³³⁶ AI Act, Article 50.

providers, when assessing systemic risks, to ‘*also focus on the information which is not illegal but contributes to the systemic risks identified in this Regulation*’ and ‘*pay particular attention on how their services are used to disseminate or amplify misleading or deceptive content, including disinformation*’.³³⁷

From the text of the Regulation, it emerges that platforms are required to address the potential dissemination of illegal or harmful content insofar as it results from the design or functioning of their services, or from the utilisation made by their users. This raises the question of whether VLOPs and VLOSEs are merely expected to ensure that they do not *facilitate* the diffusion of certain types of content (e.g., their algorithms do not inadvertently amplify certain types of content), or whether they are also required to actively intervene to remove such content.

As also discussed below,³³⁸ these obligations, being broadly formulated, do not necessarily require platforms to increase or decrease their moderation efforts. Rather, they call for a careful and justified balancing of the risks associated with both overly proactive moderation and excessively laissez-faire approaches. What is required is a reasoned justification of the chosen measures in light of the need to safeguard fundamental rights and other civic values. It should also be noted that these rules do not entail direct *liability* for the harmful content disseminated on the platform, as immunity remains applicable. They rather establish a new form of *accountability* for this type of content,³³⁹ as inadequate compliance with these obligations may only result in the application of sanctions.³⁴⁰ Ultimately, however, it is for the European Commission to assess whether the measures adopted by these major platforms are indeed adequate.

³³⁷ DSA, Recital 84.

³³⁸ See *infra*: Chapter III, Section 1.3.

³³⁹ Martin Husovec, *Principles of the Digital Services Act* (Oxford Academic 2024) 17 <<https://academic.oup.com/book/58088>> accessed 13 November 2024.

³⁴⁰ In line with Article 74 of the DSA.

The Commission's opening of proceedings and requests for information under the DSA are ambiguous on this point, as they appear to suggest that platforms are indeed expected to adopt proactive moderation measures. Notably, proceedings have been opened against X (Twitter) pursuant to Articles 34(1), 34(2), and 35(1) of the DSA, for inadequate action against illegal content and misinformation.³⁴¹ Among the contested practices is the platform's reliance on Community Notes, a collaborative, user-driven system for flagging potentially policy-violating content,³⁴² as its primary moderation tool, rather than removing or demoting such content directly. Moreover, X has also been questioned regarding its reduction of staff dedicated to moderation.³⁴³ Similarly, also TikTok³⁴⁴ and Meta³⁴⁵ have been required to explain their actions against the spreading of illegal content, particularly terrorism, violent content, hate speech, and the alleged dissemination of disinformation. These concerns have been highlighted by former commissioner Thierry Breton following the alleged proliferation of terrorist content online after the Hamas attack in Israel on October 7, 2023.³⁴⁶

³⁴¹ European Commission, 'Commission opens formal proceedings against X under the DSA' (*European Commission*, 18 December 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709> accessed 25 March 2025.

³⁴² Marc Bovermann, 'Putting X's Community Notes to the Test' [2024] *Verfassungsblog* <<https://verfassungsblog.de/putting-xs-community-notes-to-the-test/>> accessed 23 September 2025.

³⁴³ European Commission, 'Commission Requests Information from X on Decreasing Content Moderation Resources under the Digital Services Act' (*Shaping Europe's digital future | European Commission*) <<https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-x-decreasing-content-moderation-resources-under-digital-services>> accessed 24 March 2025.

³⁴⁴ Regarding its actions against the: European Commission, 'Commission Sends Request for Information to TikTok under the Digital Services Act' (*Shaping Europe's digital future | European Commission*, 19 October 2023) <<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-tiktok-under-digital-services-act>> accessed 24 March 2025.

³⁴⁵ European Commission, 'Commission Sends Request for Information to Meta under the Digital Services Act' (*Shaping Europe's digital future | European Commission*, 19 October 2023) <<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-0>> accessed 24 March 2025.

³⁴⁶ Thierry Breton [@ThierryBreton], '#TikTok Has a Particular Obligation to Protect Children & Teenagers from Violent Content & Terrorist Propaganda —as Well as Death Challenges & Potentially Life-Threatening Content. #DSA Sets out Very Clear Obligations TikTok Must Comply

While these enforcement actions seem to point towards an emerging expectation that VLOPs and VLOSEs moderate both illegal and harmful content, a different approach can be discerned in the European Commission's *Guidelines for the mitigation of systemic risks online for electoral processes*.³⁴⁷ In this document, the recommended measures include: the promotion of official information on electoral processes and of media literacy initiatives; the reduction of the virality of content that threatens the integrity of electoral processes and the explicit labelling of political advertising; the adoption of specific mechanisms linked to generative AI, which could be used to create or disseminate harmful content (such as deepfakes). It is noteworthy that in this context, the focus is placed on limiting the virality of harmful content, rather than imposing a positive obligation to remove it.

The possibility of imposing moderation duties on harmful content for online platforms has become a highly contentious geopolitical issue, when the United States have accused the European Commission of online censorship.³⁴⁸ The problem with imposing an obligation to moderate harmful content is that, unlike illegal content, which is clearly identified by national and EU law, it lacks a legal definition. This absence of definition opens the door to arbitrary decisions, effectively leaving it to the platforms themselves to identify harmful content, with

with. Letter to TikTok CEO Shou Zi Chew  <https://t.co/J1tpVzXaYR> <<https://x.com/ThierryBreton/status/171247210822329056>> accessed 27 October 2025.

³⁴⁷ Communication from the Commission, Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065, C/2024/3014. According to the DSA, the Commission, in cooperation with the national DSCs, and after conducting a public consultation, may issue guidelines in relation to specific risks and recommend possible measures.

³⁴⁸ House Judiciary Committee, 'Europe's Threat to American Speech and Innovation' <<http://judiciary.house.gov/committee-activity/hearings/europes-threat-american-speech-and-innovation>> accessed 23 September 2025.

the contribution of the EU institutions involved in the enforcement, i.e., primarily the European Commission, a highly politicised body.³⁴⁹

In this context, commissioner Virkkunen has clarified that the DSA is content-agnostic,³⁵⁰ meaning that the European Commission cannot compel platforms to moderate specific lawful content, such as all Kremlin-aligned views or vaccine criticism, even when such content may negatively affect elections or civic discourse.³⁵¹ Not only does such a power lack a legal basis in the text of the Regulation, but it would also cross a fundamental *red line* of the DSA, considering the constitutional architecture of the European Union.³⁵² In line with this interpretation, where lawful content is concerned, the Commission may, at most, enforce obligations aimed at limiting the amplification or rapid spread of *all* content with viral potential, regardless of its political orientation or message.³⁵³ Nonetheless, as the limits of Commission's power in the context of systemic risks provisions is not clear, scholars have underlined the need for a greater clarity.³⁵⁴

The question of the standard-setting power of the Commission is also linked to the possibility to promote the adoption of code of conducts. The fact that participating and complying with relevant code is considered an appropriate way to mitigate

³⁴⁹ Ilaria Buri, 'A Regulator Caught Between Conflicting Policy Objectives. Reflections on the European Commission's Role as DSA Enforcer' in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023) 85.

³⁵⁰ Pieter Haeck, 'EU Social Media Law Isn't Censorship, Tech Chief Tells US Critic' (*POLITICO*, 10 March 2025) <<https://www.politico.eu/article/social-media-law-does-not-regulate-speech-eu-tech-chief-tells-us-lawmaker-henna-virkkunen/>> accessed 23 September 2025.

³⁵¹ From Martin Husovec and et al., 'Re: Hearing on "Europe's Threat to American Speech and Innovation"' (3 September 2025) <<https://husovec.eu/wp-content/uploads/2025/09/US-Academic-Letter-DSA-Censorship.pdf>>.

³⁵² Martin Husovec, 'The Digital Services Act's Red Line: What the Commission Can and Cannot Do about Disinformation' (2024) 16 *Journal of Media Law* 47 <<https://doi.org/10.1080/17577632.2024.2362483>> accessed 23 September 2025.

³⁵³ From Husovec and et al. (n 351).

³⁵⁴ Daphne Keller, 'Comment to Council of Europe Committee of Ministers on the Draft Recommendation on Online Safety and Empowerment of Content Creators and Users' (Social Science Research Network, 8 August 2025) <<https://papers.ssrn.com/abstract=5384268>> accessed 23 September 2025.

systemic risks and to rectify infringements has raised questions about whether these codes could still be considered voluntary soft law measures.³⁵⁵ In fact, the inclusion of the Code of Practice on Disinformation and the Code of Conduct on Countering Illegal Hate Speech Online³⁵⁶ in the DSA, marked a trend toward the ‘legalisation’ of codes of conducts, with the DSA becoming a tool to apply actual sanctions in the case of non-compliance.³⁵⁷

Code of conducts and the crisis response mechanism

The DSA mentions the possibility for the European Commission and the newly established European Board of Digital Services (EBDS) to encourage the adoption of code of conducts to support the application of the DSA, particularly in the area of combating illegal content and mitigating systemic risks.³⁵⁸ The European Commission can also invite VLOPs and VLOSEs to participate in the development of code of conducts to address identified systemic risks, which may include mitigation measures and periodic reporting obligations.³⁵⁹

The participation in these instruments appears to be highly relevant for assessing compliance with systemic risk mitigation obligations borne by VLOPs and VLOSEs. Indeed, participation and compliance with a relevant code can be considered an appropriate way to mitigate systemic risks and rectify infringements.³⁶⁰ Moreover, the preamble of the DSA establishes that if a VLOP or VLOSE refuses, without proper explanation, the Commission’s invitation to participate in a code, this could be taken into account when determining whether a

³⁵⁵ Carl Vander Maelen and Rachel Griffin, ‘Twitter’s Retreat from the Code of Practice on Disinformation Raises a Crucial Question: Are DSA Codes of Conduct Really Voluntary?’ (*DSA Observatory*, 12 June 2023) <<https://dsa-observatory.eu/2023/06/12/twitters-retreat-from-the-code-of-practice-on-disinformation-raises-a-crucial-question-are-dsa-codes-of-conduct-really-voluntary/>> accessed 6 March 2025.

³⁵⁶ Already mentioned *supra*: Section: 1.3.

³⁵⁷ Maelen and Griffin (n 355).

³⁵⁸ DSA, Article 45(1).

³⁵⁹ DSA, Article 45(2).

³⁶⁰ DSA, Recital 104, Article 75(2).

DSA infringement has occurred.³⁶¹ Furthermore, once a code of conduct has been adopted, there are reporting obligations, and it is possible for an audit report to assess compliance with it.³⁶²

As a consequence, even though compliance with systemic risks obligations can be achieved through any means and mere participation in a code of conduct is not sufficient on its own, refusing to participate may entail significant risks. For this reason, some scholars have argued that, under the DSA, codes of conducts represent something more than a voluntary self-regulatory instrument, raising questions about the freedom of X (Twitter) to withdraw from the Code of Practice on Disinformation.³⁶³ In fact, in the early months of 2025, the Code of Practice on Disinformation and the Code of Conduct on Countering Illegal Hate Speech Online³⁶⁴ became officially DSA codes, thereby becoming the reference point for assessing whether VLOPs and VLOSEs adequately mitigate systemic risks.³⁶⁵

Another significant provision specifically regarding VLOPs and VLOSEs is the crisis response mechanism established under Article 36. It states that, in the event of a crisis, the European Commission may issue a decision imposing one or more platforms to assess their role in the crisis and identifying measures to address the situation. A crisis refers to exceptional circumstances posing a serious threat to public security or public health within the European Union or a part of it.³⁶⁶

³⁶¹ DSA, Recital 104.

³⁶² DSA, Article 75(4).

³⁶³ Maelen and Griffin (n 355).

³⁶⁴ Already mentioned *supra*: Section: 1.3.

³⁶⁵ European Commission, 'The Code of Conduct on Countering Illegal Hate Speech Online +' (*Shaping Europe's digital future | European Commission*, 20 January 2025) <<https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online>> accessed 21 March 2025. European Commission, 'The Code of Conduct on Disinformation' (*Shaping Europe's digital future | European Commission*, 13 February 2025) <<https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation>> accessed 21 March 2025.

³⁶⁶ DSA, Article 36(2).

This provision formalises the practice mentioned in the introduction of this chapter, highlighting the tendency to address various social crises through digital platforms. It is conceivable that triggering of this mechanism may require platforms to moderate content or to prioritise certain types of information. This mechanism effectively opens the way for the Commission to intervene on information flows on platforms in cases of emergency in the public interest. However, also in this context such interventions should be *content-agnostic*.

CONCLUDING REMARKS

The regulation of online intermediaries' role in transmitting information has traditionally been approached through the lens of liability, with a general immunity for third-party illegal content applying to them. This solution has been adopted by both the US and the EU in the late 1900s and early 2000s, with two main differences. The US law, still in force today, explicitly recognises the possibility for internet providers to engage in voluntary moderation activities, thereby fully legitimising the removal of user content in accordance with their terms of service. On the other hand, under the EU framework, immunity is conditional upon the provider's lack of knowledge of the illegality of the transmitted content or, upon becoming aware of it, the provider's prompt removal of such content.

The traditional immunity regime has been called into question over the past decade due to several developments characterising the digital space. These include the dominance of platforms engaging in pervasive content curation practices, as well as the dissemination on such platforms of content deemed harmful to society, often allegedly amplified by algorithmic recommendation systems. Within the EU legal system, the Court of Justice has repeatedly examined the qualification of platforms' content curation practices, generally upholding their immunity. Similarly, in the United States, attempts to hold platforms accountable for their filtering activities have thus far proven unsuccessful. On the other hand, academic debates have increasingly juxtaposed online platforms with traditional media bearing editorial responsibility, promoting broader accountability for content curation practices.

Within the European Union, these perspectives prompted the promotion of co-regulatory instruments for major platforms, the introduction of sector-specific obligations, and have then culminated in the adoption of the Digital Services Act in 2022. The Digital Services Act ultimately reaffirmed the immunity of digital intermediaries for user-generated content while introducing some significant innovations regarding intermediary liability. Despite a reaffirmation of the safe harbour principle, the DSA has entailed a greater accountability of digital platforms for the content transmitted, widening the cases in which they are required to act. First, an explicit Good Samaritan Protection has been established, although coupled with reporting duties for certain serious criminal activities. Second, cases of ‘mandatory’ moderation have been introduced at EU level, both at the request of judicial authorities (Art. 9) and users (Art. 16). Although these provisions entail a risk of excessive content removal by platforms in order to avoid sanctions, they have the merit of strengthening external control over the legality of online content, contributing to a greater diffusion of power in the digital public sphere. Similarly, the special prerogatives entrusted to certain actors, such as ‘trusted flaggers’ (Art. 22), help to counterbalance the hegemony of platforms, promoting a more pluralistic system.³⁶⁷ Broadly, there seem to be a growing expectation that platforms participate in law enforcement and apply legal standards in their decision making,³⁶⁸ to pursue a greater alignment with the legal order and the public interest.

In the case of VLOPs and VLOSEs, the systemic risks mitigation framework has generated debate regarding whether these provisions impose an obligation to undertake active content moderation activities, since they require to address the dissemination of illegal content, as well as wider negative impacts on civic discourse and electoral processes. However, there is an emerging consensus that these provisions do not mandate the removal of illegal or harmful content but rather

³⁶⁷ See also: Chapter III, Concluding Remarks.

³⁶⁸ Ortolani (n 20) 162.

require the adoption of measures to avoid *facilitating* or *amplifying* its spread, for example by addressing virality-enhancing mechanisms. Crucially, this obligation should be considered as content-agnostic, meaning that platforms cannot be required to de-prioritise specific topics.

More broadly, it must be noted that not all additional obligations imposed on platforms regarding illegal or harmful content are linked to enhanced liability. In many cases, a violation of the obligations set out in the Digital Services Act results in the imposition of administrative fines, signalling a shift away from the traditional binary framework of exemption versus liability, rather pursuing a broader *accountability* of digital intermediaries.³⁶⁹

From a wider perspective, considering the rapidly evolving digital landscape, it is worth wondering whether the DSA liability framework could extend to providers of generative AI systems. The traditional immunity rules were conceived for intermediary services, that is, entities transmitting third-party content without producing their own. As such, they appear only partially extendable to generative AI services, and only insofar as these systems provide access to external content. This suggests that, when elaborating their own content, providers of generative AI systems may be expected to exercise a higher degree of control over the content they disseminate, similar to editorial curation. Consequently, they could be held directly liable for such content, and the due-diligence obligations established by the DSA would likely not apply. Conversely, the AI Act does not include specific rules on content management, apart from the requirement to clearly label artificially generated outputs and *deepfakes*.³⁷⁰ Nonetheless, certain content management duties may arise indirectly from the AI Act's systemic risk assessment obligations.³⁷¹

³⁶⁹ Husovec, 'Will the DSA Work? On Money and Effort' (n 19) 21.

³⁷⁰ AI Act, Article 50.

³⁷¹ AI Act, Article 55.

A new approach has also been introduced with regard to platforms' voluntary content moderation practices: while they remain free to engage in such activities, also thanks to the introduction of an explicit Good Samaritan protection, the Digital Services Act has established several rules to frame the exercise of this power. These rules are analysed in the following chapter.

III. MODERATION ACTIVITIES: THE DSA FRAMING CONTENT RESTRICTIONS

As previously mentioned, moderation constitutes one facet of digital platforms' gatekeeping power. It consists in the removal or shading of content deemed illegal or harmful, following an order from a national authority or the service provider's own assessment. Moderation and banning practices are not new to the communication industry, as the proliferation of 'bad' content is a classical issue of public communication. Consequently, they pre-date the digital era, being part of traditional media activities.

However, the concrete forms of moderation differ across communication media. The digital platform environment has its own distinct practices, each characterised by a different level of constraint. The simplest form is content suppression, which constitutes, however, a *hard* form of moderation, resulting in a total restriction of freedom of expression. The objective pursued, akin to traditional censorship mechanisms, is to block the transmission of information, thereby hindering its reach to the public. Unlike traditional censorship, however, content removal on digital platforms generally occurs *ex post*, meaning after the content has already been published or disseminated. Consequently, its impact is limited to preventing further dissemination (i.e., to users who have not yet seen the content) and restricting subsequent access to the same illegal content (for users who have already encountered it). Content suppression, especially when performed on social media platforms, can be the first step leading to the suspension or removal of the individual user's account.³⁷² This sanction is the most severe form of moderation, and it can significantly impact various aspects of users' social and professional life.³⁷³

³⁷² MacKinnon and others (n 176) 24.

³⁷³ Gillespie (n 60) 177.

Conversely, softer remedies against harmful content that do not involve suppression include access restrictions for certain categories of users (e.g., minors), the imposition of automatic but removable filters (e.g., *SafeSearch* by Google),³⁷⁴ and demotion in rankings and recommender systems. The demotion of harmful content in ranking and recommender systems is indeed a common moderation tool. It is used to reduce users' exposure to certain type of information through its de-prioritisation within the algorithm controlling content curation on the platform. This practice, commonly referred to as *shadow-banning*,³⁷⁵ differs from systematic content recommendation practices, as addressed in Chapter IV, due to its specific moderation rationale. For this reason, while recommender systems aim to promote content that is likely to engage users, operating as a systematic and positive function, shadow banning represents a negative, exceptional intervention aimed at limiting the reach of specific content.

It must be noted that, even though shadow-banning may appear as a more lenient approach to freedom of speech, its silent nature and effectiveness make it a powerful repressive tool. As extensively demonstrated, in the Web 2.0, it can be extremely difficult to encounter information that is not prioritised unless users specifically and actively search for it (for instance, by directly accessing the URL).³⁷⁶ Moreover, users, including the author of the content itself, may not be aware or be certain about the application of such a measure, as no formal communication was typically provided. This lack of transparency undermines public debate around content suppression, while allowing platforms to avoid reputational damage and formal

³⁷⁴ Google Search, 'Filter or Blur Explicit Results with SafeSearch' (*Google Search Help*) <<https://support.google.com/websearch/answer/510?hl=en&co=GENIE.Platform%3DAndroid>> accessed 28 March 2025. A similar approach has been traditionally adopted by Tumblr, see: Gillespie (n 60) 177.

³⁷⁵ Geoffrey A Fowler, 'Perspective | Shadowbanning Is Real: Here's How You End up Muted by Social Media' *Washington Post* (27 December 2022) <<https://www.washingtonpost.com/technology/2022/12/27/shadowban/>> accessed 4 March 2025.

³⁷⁶ See *infra*: Chapter IV.

complaints. However, recent EU regulations have acknowledged the existence of these moderation mechanisms, as elaborated further below.³⁷⁷

The novelty of these techniques for content suppression and demotion is debatable. Although a comparative analysis of content curation tools across various media outlets (such as newspapers, television, and radio) falls outside the scope of this research, it is evident that each communication technology comes with its own specific characteristics. Nevertheless, recent practices such as shadow-banning may be somewhat analogous to scheduling adult-only television programs in the late-night to limit their viewership.³⁷⁸ Given that every mass communication technology inevitably gives rise to issues of misuse and the need to balance diverse sensibilities among users, certain questions surrounding moderation carry a degree of ineluctability.

As already mentioned, the activation of moderation tools in digital realm can stem from various sources. Content suppression may result from a request made by public authorities or a spontaneous action by the platform. In the first case, there is typically a violation of national regulations, meaning that the content is deemed illegal. In the second case, the platform states that the content conflicts with its terms and conditions. In this context, the content may be also illegal, but it is ultimately up to the platform to make that determination.

Intervention at the behest of national authorities concerning illegal content is closely linked to the issue of platform liability, which was addressed in the previous chapter.³⁷⁹ In this regard, the main innovation introduced by the DSA concerns the harmonisation of notice-and-action mechanisms. While this type of intervention raises concerns related to public censorship over online speech, democratic countries typically entrust independent judiciary bodies with the power to require

³⁷⁷ Reference is to the DSA, Recital 55 and Article 17, further analysed in following Section 1.2.

³⁷⁸ Gillespie (n 60) 177.

³⁷⁹ See *supra*: Chapter II.

private actors to remove illegal content, in accordance with their constitutional architecture. Consequently, the legitimacy of such public interventions over online content ultimately depends on the quality of democratic governance, the robustness of rule of law, and respect for fundamental rights in a given country. Conversely, spontaneous interventions by platforms present inherent challenges related to democracy and legitimacy.

Most online moderation activities are carried out voluntarily, based on terms and conditions of use that users are obliged to accept in order to access digital services, following a private law structure. As with any contract, these terms can establish obligations and prohibitions, as well as general clauses, such as the platform's prerogative to suppress any content not in line with the law or with the so-called *community standards*. It must be noted that these clauses are always unilaterally imposed, creating a significant asymmetry to the detriment of the user-consumer.³⁸⁰ This asymmetry is often exacerbated by the platform's dominant position in the relevant market. In practice, since major platforms do not have significant competitors, users have no real choice but accept the terms, or forgo access to the services altogether.³⁸¹ In this context, it has been highlighted how the expression 'community standards', suggesting a form of collective or bottom-up regulation, is misleading.³⁸² This notion may have held some truth in the early days of platforms like Facebook, which was initially used by a homogeneous group of Ivy League male students. However, the idea of a uniform community of values peacefully agreeing on the boundaries of public speech is unrealistic even on a small scale – and entirely unconceivable given the current global scope of platforms' activities.³⁸³

³⁸⁰ Helberger (n 80) 842.

³⁸¹ Terms and conditions of major platforms have been defined as 'boilerplate' agreement because they are contractual in form, but essentially mandatory (Cohen (n 3) 44.).

³⁸² Suzor (n 238) 39.

³⁸³ Gillespie (n 60) 118.

The fact that moderation activities on digital platforms are often governed by contract law is particularly concerning given the scale at which they operate, i.e. the number of users subject to a single private moderator.³⁸⁴ This situation recalls the early days of television, when only a few channels existed, though their scope at that time was confined to the national level. Conversely, the transnational scope of platforms' rule-making power has been compared to that of empires.³⁸⁵ Today's digital landscape raises then classic media pluralism concerns, though in a radically different context. As prominent scholars have observed, contemporary pluralism challenges no longer arise from technological scarcity (such as limited broadcast frequencies) but from the scarcity of human attention, as individuals can only process a limited amount of information.³⁸⁶

From a legal point of view, relegating content moderation to private law is a model fully legitimised by the Good Samaritan Protection provided under Section 230 of the US Communications Decency Act, which allows platforms to determine what content is objectionable and remove it, with the only limitation being the requirement of 'good faith'.³⁸⁷ In such a system, platforms – largely free from significant pressure from competitors or other external forces – unilaterally decide what can be said online and have been able to establish the boundaries of what is considered appropriate in the digital public sphere. Examples abound to illustrate this. For instance, Facebook's past systematic suppression of breastfeeding pictures was widely perceived as an attempt to label such practice as obscene and unsuitable for public spaces, in contrast with a longstanding battle fought by mothers.³⁸⁸ Similar debates have emerged concerning non-nudity pictures depicting menstrual

³⁸⁴ Gillespie (n 60) 74.

³⁸⁵ Bradford (n 2) 8.

³⁸⁶ Wu, 'Is the First Amendment Obsolete?' (n 114) 554. See also: Chapter I, Section 2.2; and Chapter IV.

³⁸⁷ See *supra*: Chapter II, Section 1.

³⁸⁸ For a detailed history of the liberalization of breastfeeding pictures on Facebook see: Gillespie (n 60) 145.

blood.³⁸⁹ Another notable case involved Facebook's repeated removal of the iconic 'Napalm Girl' photograph from the Vietnam War.³⁹⁰ Given the profound impact of this image on public perception of the United States' involvement in the war when it was published in traditional media in 1972, its suppression raised questions about the risk of such crucial information for public opinion being concealed today due to inconsistency with major platform's community standards. While these examples also underscore how pressure and public debate have been able to influence moderation rules over time; achieving such changes required significant efforts and massive mobilisation of public opinion – a feat not easily replicable for cases lacking widespread visibility.³⁹¹

Furthermore, even when platforms remove content that violates national regulation, if they do so spontaneously, they assume the authority to interpret and enforce the law. Additionally, prior to the intervention of European lawmakers, owing to the contractual nature of content moderation, there was typically no principle of legality or right of appeal.³⁹² It is also noteworthy that content moderation rules are heavily shaped by the methods used for their enforcement. Given the large volume of content to be reviewed, practical implementation plays a crucial role in defining the actual scope of restrictions. This process inherently involves a degree of arbitrariness, including biases that may arise from both human moderators and algorithmic systems.³⁹³ As a result, inaccuracies and inconsistencies frequently

³⁸⁹ Suzor (n 238) 36.

³⁹⁰ Gillespie (n 60) 1.

³⁹¹ Suzor (n 238) 37.

³⁹² Suzor (n 238) 22, 37.

³⁹³ Gillespie (n 60) 118. For further developments of the risks entailed by the use of algorithms in moderation decisions, see: Gorwa, Binns and Katzenbach (n 139).

occur, often with a disproportionate impact on already marginalised groups,³⁹⁴ perpetuating social injustices and bias.³⁹⁵

Another significant issue with online content moderation has always been its opacity. Many aspects of these activities have been uncovered only through leaks or investigative journalism.³⁹⁶ This lack of transparency may be attributed to several factors. Firstly, platforms generally wish to maintain an image of neutrality, making it preferable for moderation to operate behind the scenes. This is also due to the fact that moderation inevitably involves making contentious decisions, which can potentially harm platforms' reputation.³⁹⁷ In fact, some authors suggest that platforms have been compelled to intervene on content due to public pressure following scandals but have done so reluctantly.³⁹⁸ Nevertheless, as previously mentioned, platforms also have an economic incentive to present themselves as reliable actors.

Although digital platforms have traditionally followed a private law structure when restricting content, they frequently emphasise their commitment to protecting free speech. Despite the contested horizontal effect of freedom of expression,³⁹⁹ platforms claim to balance this freedom with other values in their content curation practices. Consequently, they generally present their moderation rules as a necessity.⁴⁰⁰ For instance, Instagram states: *'Instagram is a reflection of our diverse*

³⁹⁴ Corynne McSherry and Jillian C York, 'Content Moderation Is Broken. Let Us Count the Ways.' (*Electronic Frontier Foundation*, 29 April 2019) <<https://www.eff.org/deeplinks/2019/04/content-moderation-broken-let-us-count-ways>> accessed 8 April 2025.

³⁹⁵ Naomi Appelman, 'Research Report on Disparate Content Moderation' (*DSA Observatory*, 31 October 2023) <<https://dsa-observatory.eu/2023/10/31/research-report-on-disparate-content-moderation/>> accessed 6 March 2025.

³⁹⁶ Some obscure aspects of content moderation have for instance been published by a Wall Street Journal investigation known as 'The Facebook Files': Jeff Horwitz and others, 'The Facebook Files' *Wall Street Journal* (1 October 2021) <<https://www.wsj.com/articles/the-facebook-files-11631713039>> accessed 4 March 2025.

³⁹⁷ Suzor (n 238) 47.

³⁹⁸ On Google Search: Gillespie (n 60) 185.

³⁹⁹ De Gregorio (n 165) 188.

⁴⁰⁰ Gillespie (n 60) 47.

community of cultures, ages, and beliefs. We've spent a lot of time thinking about the different points of view that create a safe and open environment for everyone. We created the Community Guidelines so you can help us foster and protect this amazing community'.⁴⁰¹ Balancing freedom of expression and the inhibition of offensive content is a long-standing issue. Despite the dissemination of content being protected in all democracies by the freedom of speech, it is generally acknowledged that this freedom is subject to certain limitations.⁴⁰² Indeed, the very same democratic values may sometimes require restrictions on free speech. This balancing act raises complex questions, such as whether restrictions should be confined to what is illegal or extend to what is merely inappropriate, and whether private entities have duty to respect free speech. The sensitivity of this balance has been exemplified by cases such as the banning of Donald Trump's account from Twitter.⁴⁰³

Typically, the boundaries of freedom of expression are addressed by legislators and courts, especially constitutional courts, which are primarily entrusted with the duty to protect and balance conflicting fundamental rights. Given their scale and the

⁴⁰¹ Accessible here: Meta, 'Community Standards' (*Meta | Transparency Centre*) <<https://transparency.meta.com/policies/community-standards/>> accessed 26 October 2025. This kind of representation is similar in all platforms. X: "*X's purpose is to serve the public conversation. Violence, harassment and other similar types of behavior discourage people from expressing themselves, and ultimately diminish the value of global public conversation. Our rules are to ensure all people can participate in the public conversation freely and safely*" (X, 'The X Rules: Safety, Privacy, Authenticity, and More' <<https://help.x.com/en/rules-and-policies/x-rules>> accessed 26 October 2025.); TikTok: '*We have Community Guidelines to help keep TikTok a safe and positive experience*' (TikTok, 'Community Guidelines: Overview' (*TikTok*) <<https://www.tiktok.com/community-guidelines/en/>> accessed 26 October 2025.)

⁴⁰² However, the American tradition is less inclined to accept restrictions on freedom of expression, which is protected by the First Amendment of the U.S. Constitution. In fact, the dominant metaphor in the discourse was the one of the 'marketplace of ideas' (famously endorsed by the Supreme Court Justice Holmes in 1919) according to which if all voices can speak, the better ones will emerge. See: Maroni and Brogi (n 232) 18; Giovanni De Gregorio, 'Il Diritto Delle Piattaforme Digitali: Un'analisi Comparata Dell'approccio Statunitense Ed Europeo al Governo Della Libertà Di Espressione' (2021) 50 DPCE Online <<https://www.dpceonline.it/index.php/dpceonline/article/view/1531>> accessed 9 October 2025; Schepisi (n 11).

⁴⁰³ See *supra*: Chapter I, Section 1.2.

ability to determine what is acceptable in a considered society, the balancing act performed by Big Tech between freedom of expression and potentially harmful content is comparable to the work of constitutional courts, but without the same legitimacy. On the other side, it must also be acknowledged that entrusting all disputes regarding harmful content online to the courts would entail accepting a posthumous and belated intervention, inefficient in terms of protecting the interests at stake. That said, European lawmakers chose not to prevent digital intermediaries from moderating content, but rather to counterbalance their power. As a result, the Digital Services Act dedicates numerous provisions to moderation activities, introducing several transparency obligations and procedural safeguards. These new rules are presented in the first section of this chapter (Section 1). Moreover, the European Media Freedom Act has strengthened these safeguards when moderation targets media service providers, with the aim of protecting freedom of the press. The provisions relating to moderation practices toward media services introduced by this Regulation are outlined and discussed in subsequent Section 2.

1. THE DSA’S FRAMEWORK ON MODERATION ACTIVITIES

The regulation of moderation practices spontaneously conducted by online intermediaries represents one of the major contributions of the DSA. The relevant provisions recall the primary objectives of the entire regulation, i.e. fostering individual fundamental rights in the digital sphere. This is pursued by introducing safeguards for users’ freedom of speech through transparency obligations and due process mechanisms.⁴⁰⁴

Before presenting these rules, it is useful to briefly recall some of the provisions analysed in the previous chapter, which help to frame the broader picture regarding platforms’ moderation activities. First of all, in continuity with the ECD, hosting providers are generally exempt from liability for third-party illegal content,

⁴⁰⁴ Husovec, ‘Will the DSA Work? On Money and Effort’ (n 19) 22.

meaning they are not subject to a general obligation to moderate or monitor users' activities on their services. However, such exemption is conditional, as it is lost whenever the provider becomes aware of the illegality of the content and fails to remove it. Under the DSA and in line with previous CJEU case law, a provider can be deemed aware – and therefore liable – for illegal content when it receives a sufficiently precise and reasoned notification from public authorities or users. In such cases, mandatory moderation arises. Additionally, the DSA introduces further due diligence obligations for platforms designated as VLOPs or VLOSEs in the context of systemic risk mitigation obligations, which may also extend to merely 'harmful' content.⁴⁰⁵

On the other side, with regard to spontaneous moderation activities, the DSA introduces an explicit Good Samaritan clause,⁴⁰⁶ establishing that liability exemption is not lost when a platform voluntarily removes illegal content. However, in accordance with Article 18 of the DSA, when a hosting provider becomes aware of serious illegal content during such voluntary activities, it is required to notify the competent public authorities.

Notably, the EU version of the Good Samaritan protection explicitly covers only the removal of illegal content – not content that is merely inconsistent with platforms' terms and conditions. However, the spontaneous moderation of non-illegal content based on the terms of the service is widespread in the current digital environment. As previously discussed, through these contractual clauses, platforms arrogate to themselves the right to suppress content that does not align with their internal standards. This may include non-illegal content such as nudity, disinformation or hate speech – generally grouped under the broad label of 'harmful' content.⁴⁰⁷ Even though such moderation activities are not covered by

⁴⁰⁵ See *supra*: Chapter II, Section 2.4.

⁴⁰⁶ DSA, Article 7.

⁴⁰⁷ In some countries they are illegal, but not in every country. For instance, in Italy, hate speech that does not qualify as propaganda or incitement to violence is not considered a criminal offense.

Article 7, they appear to be equally legitimised under the DSA framework, since transparency obligations and procedural safeguards explicitly apply to them. Consequently, it is possible to affirm that platforms are generally authorised to remove content deemed harmful, but they are not required to do so.

The regulation of spontaneous moderation practices under the DSA follows the system of escalating obligations depending on the type and size of the intermediary, which was presented in the previous chapter.⁴⁰⁸ Consequently, certain obligations apply to all intermediaries, while additional, enhanced duties are imposed on specific categories. The analysis of the relevant rules will be structured as follows. First, transparency obligations relating to moderation activities are examined (Section 1.1), followed by an analysis of due process obligations in connection with content restrictions decision (Section 1.2), to finally address the obligations to respect users' fundamental rights in the context of moderation practices (Section 1.3).

1.1. TRANSPARENCY OBLIGATIONS ON MODERATION ACTIVITIES

The first category of rules concerning moderation activities imposes transparency obligations on intermediary service providers. These transparency obligations can be divided into two types: *ex ante* obligations, requiring providers to clearly provide information about moderation policies in their terms of services, and *ex post* obligations, requiring them to periodically report on the moderation activities they have performed.

Transparency of terms and conditions on moderation policies

The first transparency obligation introduced by the DSA concerns the clarity and accessibility of providers' terms of service (ToS), with particular emphasis on the disclosure of content moderation policies and procedures. This obligation applies to all intermediaries, which, pursuant to Article 14(1) of the DSA, must provide

⁴⁰⁸ See *supra*: Chapter II, Section 2.1

clear information regarding content restriction in their terms and conditions of use. This includes details on policies, procedures, and tools; the use of algorithmic decision-making and human oversight; and rules governing existing complaint mechanisms. Any significant modification of the terms and conditions must also be communicated to users.⁴⁰⁹ This information must be presented in clear and intelligible language, be publicly accessible, and have a user-friendly format. Services primarily directed at minors or predominantly used by them must explain their terms and conditions on restrictions in a way that minors can understand.⁴¹⁰ In addition to this, VLOPs must provide for a concise, easily accessible and machine-readable summary of their terms.⁴¹¹

These rules can be seen as introducing a form of legality principle in spontaneous moderation practices, meaning that users must be made aware in advance of the restrictions they may encounter when using the service. Although Article 14 does not explicitly invalidate restrictions that are not clearly communicated in the terms of services, subsequent Article 15 and Article 17 lends support to this interpretation. According to Article 15, providers are required to disclose the type of harmful conduct associated with restrictions in transparency reports.⁴¹² Moreover, as discussed further below, Article 17 requires hosting providers to precisely identify the contractual clause that has been violated by the user when applying a restriction.⁴¹³ In this sense, the DSA can be seen as implicitly conditioning the legitimacy of spontaneous moderation practices on prior transparency and clear contractual grounding, thereby reducing arbitrariness in moderation activities.⁴¹⁴

⁴⁰⁹ DSA, Article 14(2).

⁴¹⁰ DSA, Article 14(3).

⁴¹¹ DSA, Article 14(5).

⁴¹² DSA, Article 15(c).

⁴¹³ DSA, Article 17(3)(e).

⁴¹⁴ The case-law from some Member States (such as Germany) ordering the reinstatement of non-illegal content that was removed because of the alleged violation of vague terms and conditions could be further strengthened after the entry into force of the Digital Services Act (Aleksandra Kuczerawy, 'Remedying Overremoval' in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023) 175.)

Moreover, with regard to the formulation of terms of service, the European Commission has explained on its website that this measure is meant to make it easier for users to understand what they are agreeing to, without having to scroll through pages of dense and complex terms of service,⁴¹⁵ especially on VLOPs.

The second type of transparency obligations relates to the publication of periodic reports on moderation activities. This duty applies to all intermediaries, although additional reporting requirements are foreseen for to specific categories of providers.

Transparency reports on moderation activities

With regard to the reporting rules applicable to all intermediaries, Article 15 requires the publication of annual reports on content moderation activities they have carried out. These reports must include information on, *inter alia*:

- a) injunctions received from national authorities (including those based on Article 9 and 10 of the DSA), together with their rationale and the actions taken in response;
- b) spontaneous content moderation activities, including the use of automated tools, the number and type of restrictions applied, classified by type of illegality or by type of violation of terms and conditions;
- c) complaints received concerning content restriction decisions;
- d) use of automated tools for content moderation, including their qualitative description, indicators of accuracy and error rates, and any safeguard applied;
- e) for hosting providers: the number of notices of illegal content received from users through reporting mechanisms⁴¹⁶ and submissions by trusted

⁴¹⁵ European Commission, 'DSA: Making the Online World Safer | Shaping Europe's Digital Future' (*European Commission | Digital Strategy*) <<https://digital-strategy.ec.europa.eu/en/policies/safer-online>> accessed 8 October 2025.

⁴¹⁶ DSA, Article 16.

flaggers,⁴¹⁷ both classified by type of illegal content; the actions taken in response, specifying whether these were based on illegality or inconsistency with terms and conditions; the number of notices processed using automatic tools; and the median time required to take action.

Furthermore, VLOPs and VLOSEs are subject to additional reporting obligations. First, they are required to publish these reports every six months rather than annually. Second, the reports must include information on the number of human resources involved in moderation, their qualification and linguistic expertise, as well as indicators of the accuracy of the automation tools used for content moderation.⁴¹⁸

Opacity has long been one of the central issues surrounding platforms' content moderation activities.⁴¹⁹ Transparency reports on content restrictions were already published voluntarily by major platforms. However, in the absence of a common standard, these reports were not comparable across services.⁴²⁰ Moreover, they carried a significant risk of cherry-picking, as platforms could disclose only the information that did not harm their reputation. For examples, for a long time such reports focused exclusively on restrictions imposed at the request of public authorities, while omitting those applied under the platforms' own policies.⁴²¹

The list of reporting requirements is extensive, and for the average user, it may be difficult to navigate all the information provided. Nonetheless, this transparency tool, together with other disclosure obligations introduced throughout the DSA, is

⁴¹⁷ DSA, Article 22.

⁴¹⁸ DSA, Article 42.

⁴¹⁹ Suzor (n 238) 47.

⁴²⁰ MacKinnon and others (n 176) 27.

⁴²¹ MacKinnon and others (n 176) 88. Interestingly, such reports have illustrated how spontaneous moderation practices largely overcome 'mandatory' moderation, challenging the narrative about the censorship effects of the new EU regulations, particularly fostered by Trump administration (Euractiv, 'EXCLUSIVE: US Limits Free Speech More than the EU, Says Tech Commissioner' (*Euractiv*, 28 May 2025) <<https://www.euractiv.com/news/exclusive-us-limits-free-speech-more-than-the-eu-says-tech-commissioner/>> accessed 22 October 2025.)

crucial for enabling public oversight of moderation activities. Standardised and mandatory detailed reporting not only fosters accountability and promotes evidence-based public debate on online content moderation, but also generates valuable information for policymakers, potentially informing the development of future regulatory measures.

In addition to transparency obligations, intermediaries qualifying as hosting providers are subject to some other rules related to content moderation activities. These include: **(a)** providing motivation in the case of restrictions;⁴²² **(b)** introducing flagging mechanisms to allow users to notice problematic content;⁴²³ **(c)** notifying to public authorities when having suspects of a commission of a crime involving a threat to the life or safety.⁴²⁴ These constraints are further specified to what concerns host providers which may be classified as platforms: **(d)** in addition to motivation, they must establish an internal system of complaint-handling against moderation decisions⁴²⁵ and accessibility to an out-of-court dispute settlement;⁴²⁶ **(f)** in addition to notice mechanisms, they must introduce trusted flaggers systems, whose notices shall be given priority and decided without undue delay.⁴²⁷ While some of these rules introduce additional moderation duties and have therefore been already examined in the previous chapter, the following section focuses on the new procedural rules for content moderation activities.

1.2. DUE PROCESS OBLIGATIONS FOR CONTENT RESTRICTIONS: STATEMENT OF REASONS AND REDRESS MECHANISMS

For certain categories of intermediary services providers, the DSA imposes procedural duties when performing moderation activities. These include the obligation to provide a statement of reasons for content restrictions (Article 17),

⁴²² DSA, Article 17.

⁴²³ DSA, Article 16. See *supra*: Chapter II, Section 2.3.

⁴²⁴ DSA, Article 18. See *supra*: Chapter II, Section 2.2.

⁴²⁵ DSA, Article 20.

⁴²⁶ DSA, Article 21.

⁴²⁷ DSA, Article 22. See *supra*: Chapter II, Section 2.3.

which applies to all hosting providers, and specific rules on redress mechanisms (Article 20 and 21), which only apply to online platforms. It is worth noting here – though a more detailed analysis will follow – that the recently approved Media Freedom Act strengthens both the right to receive a statement of reasons and the right to appeal when the recipient of a restriction on a VLOP qualifies as media service provider.⁴²⁸

The obligation to state reasons when applying restrictions on content

The DSA mandates intermediaries qualifying as hosting providers the obligation to issue a statement of reasons when a content restriction is applied. This explanation must be provided no later than the date the restriction is imposed and applies to the following moderation techniques:

- a)* any restriction on the visibility of information provided by users, including removal of content, disabling access to content or demoting content;
- b)* suspension, termination, or other restriction of monetary payments;
- c)* suspension, termination, or limitation of the provision of the service;
- d)* suspension or termination of user accounts.

Article 17 then specifies the minimum content of such notice, which must include: the type of restriction imposed; the facts underlying the decision, including the existence of a notice submitted by another user through reporting mechanisms; the use of automated tools; in case of illegal content, the legal ground relied upon; or in case of violation of terms and conditions, a reference to the allegedly violated clause. This obligation does not apply to content restrictions performed following an order transmitted in line to Article 9 of the DSA.⁴²⁹

⁴²⁸ EMFA, Article 18. See *infra*, Section 2.

⁴²⁹ DSA, Article 17(5).

Notably, demotion in ranking and recommender systems (i.e., shadow-banning) is explicitly covered by this article.⁴³⁰ As discussed earlier, this kind of restriction has traditionally occurred without the user's awareness. With the introduction of the obligation to provide an explanation, hosting providers and platforms must now communicate the application of de-prioritisation measures.⁴³¹ This represents a significant advancement for protecting freedom of expression, also because all hosting providers are now required to precisely identify the source of illegality or the specific contractual clause that has been violated. As a result, it will become more difficult to justify arbitrary or generalised demotions in recommender systems. Although not explicitly referenced, the general obligations of transparency and access to complaint-handling systems should also apply to these forms of moderation. Nonetheless, it may still be challenging for the average user to detect and demonstrate this type of restriction.⁴³²

More broadly, the obligation imposed on hosting providers to issue a statement of reasons when applying content restrictions constitutes an undeniable progress achieved by the DSA in the context of platforms' control on information flows. The lack of explanation was one of the most problematic aspects of platforms' moderation power, contributing to its opacity.⁴³³ Although some platforms had

⁴³⁰ DSA, Article 14(1)(a) and Recital (55).

⁴³¹ Except for deceptive high-volume commercial content disseminated through intentional manipulation of the service (same article).

⁴³² In late 2023, there have been many accusations directed to Meta platforms on silent shadow-banning concerning news related to Palestine. The issue is addressed in the above-mentioned Human Rights Watch report and, *ex multis*: Kari Paul, 'Instagram Users Accuse Platform of Censoring Posts Supporting Palestine' *The Guardian* (18 October 2023) <<https://www.theguardian.com/technology/2023/oct/18/instagram-palestine-posts-censorship-accusations>> accessed 7 January 2025. In that period, the relevant DSA provisions had not yet come into force, but this situation would be now punishable. One of the first known cases in which a court found that a social media platform had violated the DSA for failing to inform a user that they were subject to a shadow-banning practice can be found here: Paddy Leerksen, 'The DSA's First Shadow Banning Case' (*DSA Observatory*, 6 August 2024) <<https://dsa-observatory.eu/2024/08/06/the-dsas-first-shadow-banning-case/>, <https://dsa-observatory.eu/2024/08/06/the-dsas-first-shadow-banning-case/>> accessed 22 January 2025.

⁴³³ Suzor (n 238) 13.

progressively improved their communication practices on content restriction, these remained largely unsatisfactory.⁴³⁴ The DSA now specifies the minimum content such notices must contain, thereby strengthening users' right to a defence. Indeed, knowing the legal grounds behind a restriction is essential for assessing its validity and enabling both individual contestation and broader societal scrutiny.⁴³⁵

To the extent that platforms are concerned, the obligation to provide a statement of reasons is coupled with the recognition of a form of right of appeal, the features of which are outlined in the next paragraph.

Accessibility to redress mechanisms against decisions on restrictions and the right to human review

Online platforms are subject to a newly introduced obligation to grant users access to redress mechanisms for contesting content restrictions, thereby conferring on them a form of right of appeal. This right may now be exercised through internal complaint-handling mechanisms, out-of-court dispute settlement bodies, and judicial redress in accordance with the laws of the relevant Member State. While the availability of judicial remedies is still dependent on national law,⁴³⁶ the DSA now institutionalises the first two avenues. Moreover, users also have the possibility to lodge a complaint before their national Digital Services Coordinator under Article 53 whenever they believe that a provider has infringed one of the DSA's provisions.⁴³⁷

The obligation for online platforms to provide users with access to an effective internal complaint-handling mechanism is established by Article 20 of the DSA. This type of remedy must be accessible for a minimum period of six months

⁴³⁴ Gillespie (n 60) 149.

⁴³⁵ Maroni and Brogi (n 232) 171.

⁴³⁶ Even though Article 54 of the DSA enshrines for service recipients a right to compensation for infringements of the Regulation.

⁴³⁷ The accessibility of these redress mechanisms is closely linked to the question of the DSA enforcement, which will be further analysed in Chapter V.

following any decision to restrict content made by the platform. It applies both to users whose content has been restricted and to users who submitted a report under Article 16. The system put in place by the platform must enable complaints to be submitted electronically, be free of charge, easily accessible, user-friendly and allow users to formulate sufficiently precise complaints.⁴³⁸ Once submitted, complaints must be handled in a timely, non-discriminatory, diligent, and non-arbitrary manner. If the complaint is deemed well-founded, the platform's original decision must be reversed. Platforms must notify users of their reasoned decision without undue delay and must also inform them of the possibility of accessing out-of-court dispute settlement. In addition to this, the DSA explicitly states that the final decision must not be based solely on automated means.

The right for users to access out-of-the-court dispute settlement bodies (ODS) to resolve dispute concerning moderation decisions is established by Article 21(1) of the DSA. These bodies are competent for the same categories of users and decisions as internal complaint-handling mechanisms and can be accessed either after an unsatisfactory referral through the internal complaint-handling mechanisms or independently. Platforms are required to publish clear information about the availability of this type of remedy. In principle, platforms are obliged to accept referrals to designated ODS bodies, unless the same case has already been treated. However, ODS decisions are not binding, even if platforms are required to cooperate in good faith.⁴³⁹

Certification of ODS bodies is granted by the Digital Services Coordinator (DSC) of the Member State where the body is established, initially for a period of five years, renewable thereafter. Certification is based on criteria such as independence,

⁴³⁸ TikTok and Meta have been recently found in compliance with such obligations (European Commission, 'DSA - Commission Preliminarily Finds TikTok and Meta in Breach of Their Transparency Obligations' (*European Commission*, 24 September 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2503> accessed 26 October 2025.)

⁴³⁹ DSA, Article 21(2).

expertise, accessibility, efficiency, and the existence of clear and fair procedural rules. Member States may also establish new out-of-court dispute settlement bodies or provide support to existing ones. The Regulation further outlines the conditions and procedures for the withdrawal of certification. Once certification is granted, the DSC must inform the European Commission, which maintains a publicly accessible list of all certified ODS bodies across Member States. Certified bodies must publish annual reports containing data on dispute outcomes, average resolution times, and any difficulties encountered. In turn, each competent DSC must publish a biennial report on the activities of ODS bodies within its jurisdiction, including best practices and recommendations.

Certified bodies are expected to issue decisions no later than 90 days after receiving a complaint, with the possibility of extending this deadline to 180 days for particularly complex cases. The DSA provides that access to these bodies must be free of charge for users or subject only to a nominal fee. For platforms, the financial contribution must be reasonable and, in any event, may not exceed the actual costs incurred by the dispute settlement body. Anyhow, if the outcome favours the user, the platform must reimburse any fees charged for the procedure. Conversely, if the platform prevails, the user is not required to reimburse costs, except in cases of bad faith.

The necessity of providing effective remedies in cases of content restrictions imposed by online platforms has long been recognised by international human rights organisations.⁴⁴⁰ Major platforms have a well-documented history of offering either no response or inadequate response to users seeking to challenge moderation decisions,⁴⁴¹ often relying on automated or standardised replies. The obligation to

⁴⁴⁰ See: Committee of Ministers Council of Europe, ‘Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the Roles and Responsibilities of Internet Intermediaries, Adopted by the Committee of Ministers on 7 March 2018 at the 1309th Meeting of the Ministers’ Deputies’ <<https://rm.coe.int/1680790e14>>.

⁴⁴¹ Suzor (n 238) 37.

establish both internal and external redress mechanisms, together with the right to receive a statement of reasons, represents a significant step toward addressing the problem of due process in platform governance. Indeed, the lack of procedural safeguards has been identified by many as the core deficiency of content moderation online.⁴⁴² Procedural safeguards are particularly important as they serve to constrain the discretionary power of platforms and reduce the risk of arbitrary decision-making.

However, some may argue that internal complaint-handling mechanisms lack effectiveness due to the absence of independence and impartiality. As previously noted, platforms simultaneously engage in rulemaking, enforcement and adjudication. In this context, regulatory provisions mandating a certain degree of internal independence in complaint-handling systems might have been desirable. Nevertheless, the availability of impartial ODS bodies helps to partially mitigate these concerns. In addition, users retain the right to bring cases before national courts, although this option may involve substantial costs in terms of both time and financial resources.

Focusing on ODS bodies, they represent a promising institutional innovation in the context of moderation activities, specifically designed to offer an independent review of platform decisions while ideally serving as a more efficient and cost-effective alternative to judicial redress. If implemented effectively, this system could help ensure that platform decision-making is subject to meaningful scrutiny and that users have a practical avenue for redress. However, the fact that decisions are not binding raises legitimate doubts about its actual impact. Past experience has shown that alternative dispute resolution risks becoming ineffective, when one of the parties lacks sufficient incentive to participate in the procedure or comply with its outcome.⁴⁴³ In this regard, the original DSA proposal was significantly bolder,

⁴⁴² Suzor (n 238) 10.

⁴⁴³ Ortolani (n 20) 159.

as it envisaged that platforms would be bound by the decisions of ODS bodies.⁴⁴⁴ This approach was later rejected, largely due to concerns about establishing extra-judicial bodies,⁴⁴⁵ with the power to adjudicate on matters involving fundamental rights.⁴⁴⁶ Nevertheless, Article 21 can still be criticised for introducing an additional layer of ‘private’ negotiability over matters of free speech and content governance.⁴⁴⁷

In the absence of a binding mechanism, the actual impact of these bodies is likely to depend on the extent to which users choose to engage with them, since widespread user recourse could generate substantial pressure on platforms to comply with their recommendations.⁴⁴⁸ Furthermore, compliance with ODS decisions may be viewed as part of the systemic risk mitigation obligations imposed on VLOPs under Article 35.⁴⁴⁹ In such a scenario, ODS bodies could become fully integrated in the DSA’s broader enforcement ecosystem. Another important aspect concerns the scope of review granted to ODS bodies, which remains ambiguous. Indeed, it is not yet clear whether they are expected to assess only procedural compliance or also the substantive merits of moderation decisions.⁴⁵⁰ Clarifying this distinction is crucial to understanding their potential role in meaningfully

⁴⁴⁴ Article 18(1) of 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 final. This proposal was criticised as it would have created extra-judicial bodies (Kuczerawy (n 414) 177.)

⁴⁴⁵ Kuczerawy (n 414) 177.

⁴⁴⁶ Such question was raised for instance in: Jörg Wimmers, ‘The Out-of-Court Dispute Settlement Mechanism in the Digital Services Act: A Disservice to Its Own Goals’ (2021) 12 JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 381, 399 <<https://www.jipitec.eu/jipitec/article/view/332>> accessed 20 May 2025.

⁴⁴⁷ This critique is connected to some concerns related to the Media Freedom Act and its ‘soft’ enforcement framework (see *infra*, Section 2.2).

⁴⁴⁸ Hannah Ruschemeier and others, ‘Brave New World. Out-Of-Court Dispute Settlement Bodies and the Struggle to Adjudicate Platforms in Europe.’ [2024] Verfassungsblog <<https://verfassungsblog.de/ods-dsa-user-rights-content-moderatin-out-of-court-dispute-settlement/>> accessed 10 April 2025.

⁴⁴⁹ Ortolani (n 20) 160.

⁴⁵⁰ Ruschemeier and others (n 448).

shaping platform moderation practices,⁴⁵¹ ultimately helping to counterbalance the unilateral power currently exercised by platforms.

Some of these bodies have already been certified, offering early indications of their characteristic. The first four designation occurred in Hungary, Malta, Germany, and Ireland.⁴⁵² Notably, variation has emerged in their geographical reach (national vs EU-wide), the platforms they supervise, fee structures, and procedural rules.⁴⁵³ These bodies have already received a significant number of cases, some submitted repeatedly by the same applicants, suggesting the emergence of regular private enforcers.⁴⁵⁴ Indeed, access to these mechanisms is open to third parties, not just the users directly affected.⁴⁵⁵ Furthermore, many ODS bodies have reported active engagement from platforms, making them a promising tool for dispute resolution in moderation decisions.⁴⁵⁶ In several instances, platforms reversed moderation decisions immediately upon being notified of an ODS procedure, due in part to the possibility of a reduced fee in such cases. However, this dynamic may create incentives for both content under-removal and over-removal,⁴⁵⁷ raising question about the effects of these mechanisms on the consistency and fairness of content moderation practices.

Another significant aspect addressed throughout the DSA is the regulation of automated decision-making. The DSA introduces transparency obligations to inform users whether decisions affecting them are made by humans or through automated means.⁴⁵⁸ Transparency reports must also include information on the use

⁴⁵¹ Ruschemeier and others (n 448).

⁴⁵² Daniel Holznagel, 'Art. 21 DSA Has Come to Life' [2024] Verfassungsblog <<https://verfassungsblog.de/art-21-dsa-fundamental-rights-certification/>> accessed 15 May 2025.

⁴⁵³ Holznagel (n 452) 1–3.

⁴⁵⁴ Holznagel (n 452) 5.

⁴⁵⁵ Giovanni De Gregorio and Simona Demkova, 'The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe' *European Yearbook of Constitutional Law* 2024 (2024) <https://link.springer.com/chapter/10.1007/978-94-6265-647-5_10> accessed 20 May 2025.

⁴⁵⁶ Holznagel (n 452) 1.

⁴⁵⁷ Holznagel (n 452) 6.

⁴⁵⁸ DSA, Article 16(6), and Article 17(3)(c).

and proportion of automation in moderation processes, both for the detection of illegal content and for the application of content restrictions.⁴⁵⁹ With respect to complaint-handling systems, the DSA explicitly states that decisions on complaints must not be made solely through automated means.⁴⁶⁰ This introduces a right to human review for moderation decisions. In effect, while automation may be used to detect potentially illegal or harmful content and to trigger restriction mechanisms, a human must ultimately validate the outcome following the submission of a complaint. It is noteworthy that these principles are becoming increasingly consolidated within EU technology regulation: they were already envisaged by the GDPR under Article 22, but the need of transparency regarding automated decision-making and the right to human oversight in critical decisions is also reflected in the AI Act,⁴⁶¹ and in the Platform Work Directive.⁴⁶²

The previous sections analysed new transparency rules and procedural obligations related to content moderation activities. To complete the overview of the new regulatory framework governing content moderation, the following section turns to the examination of the general requirements to respect fundamental rights in the context of content restrictions.

1.3. THE NEED TO RESPECT FUNDAMENTAL RIGHTS IN MODERATION ACTIVITIES

Consistent with the DSA's overarching objective of aligning platform governance with European values, the Regulation imposes on intermediary providers an obligation to respect fundamental rights in the context of moderation activities. This obligation applies to all intermediary providers under Article 14(4). In addition, a further duty is specifically imposed on VLOPs and VLOSEs, requiring them to take

⁴⁵⁹ DSA, Article 15(1).

⁴⁶⁰ DSA, Article 20(6).

⁴⁶¹ AI Act, Article 14.

⁴⁶² Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving working conditions in platform work, Article 9 and 10.

fundamental rights into account in the design and operation of their systems as part of their systemic risk management obligations.

Fundamental rights and terms of service

The aforementioned Article 14 of the DSA, which regulates the terms and conditions of service, requires intermediaries to act in a diligent, objective, and proportionate manner when applying restrictions. In doing so, they must take into account rights and legitimate interests of all parties involved, including freedom of expression, media freedom, media pluralism, and other fundamental rights of recipients as established by the EU Charter of Fundamental Rights.⁴⁶³

This open-ended provision raises several questions. On the one hand, it acknowledges, and thereby legitimise, the balancing act that platforms perform between competing fundamental rights when implementing content restrictions. By broadly referring to an obligation to respect fundamental rights and proportionality, the DSA can be seen as leaving significant discretion in the hands of platforms. This development fits within the broader trend of the ‘privatisation’ of Internet governance,⁴⁶⁴ whereby private actors are entrusted with adjudicational or policing functions traditionally exercised by public authorities.⁴⁶⁵ On the other hand, this clause allows public authorities to assess the consistency of moderation policies and decisions with fundamental rights standards. In this sense, Article 14 has been

⁴⁶³ DSA, Article 14(4).

⁴⁶⁴ Caroline Cauffman and Catalina Goanta, ‘A New Order: The Digital Services Act and Consumer Protection’ (2021) 12 *European Journal of Risk Regulation* 758, 768 <<https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/new-order-the-digital-services-act-and-consumer-protection/8E34BA8A209C61C42A1E7ADB6BB904B1>> accessed 13 November 2024.

⁴⁶⁵ Catalina Goanta and Pietro Ortolani, ‘Unpacking Content Moderation: The Rise of Social Media Platforms as Online Civil Courts’ (Social Science Research Network, 22 November 2021) <<https://papers.ssrn.com/abstract=3969360>> accessed 15 September 2025; Giancarlo Frosio, ‘Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy’ (Social Science Research Network, 6 February 2017) <<https://papers.ssrn.com/abstract=2912272>> accessed 13 November 2024.

interpreted as introducing fundamental rights obligations into the realm of content moderation, thereby conferring them a horizontal effect.⁴⁶⁶ In other words, thanks to this provision, platforms are now subject to a general legal duty to respect fundamental rights when moderating content.⁴⁶⁷ While several major platforms already declared to take into account widely-recognised fundamental rights standards,⁴⁶⁸ this constitutes now an enforceable obligation. According to the preamble of the DSA, this duty encompasses not only the rights enshrined in the EU Charter of Fundamental Rights, but also broader international standards, including the UN Guiding Principles on Business and Human Rights.⁴⁶⁹

However, the vagueness of this provision makes it difficult to determine its actual scope. How this obligation will be interpreted and enforced remains uncertain. Public authorities might, for instance, go so far as to scrutinise the content of terms and conditions themselves, potentially finding that certain justifications for restrictions are disproportionate. This interpretation is supported by the preamble of the Regulation, which states that although the contractual freedom of service providers must be respected, regulating terms of services – including provisions governing their *content* – is necessary to protect users and prevent arbitrary or unfair decisions.⁴⁷⁰ Such an interpretation has a disruptive potential, as it would enable public oversight on the contractual rules that govern online speech.

⁴⁶⁶ João Pedro Quintais, Naomi Appelman and Ronan Fahy, ‘Using Terms and Conditions to Apply Fundamental Rights to Content Moderation’ (Social Science Research Network, 25 November 2022) <<https://papers.ssrn.com/abstract=4286147>> accessed 22 January 2025.

⁴⁶⁷ A sectorial obligation was already present in the Terrorist content directive: Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, Article 5.

⁴⁶⁸ Meta’s Oversight Board, for instance, underwent a human rights assessment. See: Brent Harris, ‘An Update on Building a Global Oversight Board’ (*Meta Newsroom*, 12 December 2019) <<https://about.fb.com/news/2019/12/oversight-board-update/>> accessed 8 October 2025.

⁴⁶⁹ DSA, Recital 47.

⁴⁷⁰ DSA, Recital 45.

Alternatively, public authorities may limit their oversight to how restrictions are implemented in practice, focusing on single cases and the balancing act performed by providers in specific contexts. It is also possible that this provision will receive little attention in enforcement. In fact, its interpretation may vary significantly from one Member State to another, given that enforcement is generally in the hands of the Digital Services Coordinator of the country where the service is established and that users may also seek the application of this rule before national courts.⁴⁷¹

The lack of precision in this provision has drawn criticism. If platforms are to retain broad discretion in defining what constitutes ‘harmful’ content, and therefore what qualifies as a legitimate basis for restricting speech, then, at the very least, the DSA could have explicitly introduced a requirement to calibrate the severity of the restriction to the seriousness of the violation. For example, rather than deleting controversial content that does not pose a serious harm, platforms could have been required to apply softer measures, such as flagging or demotion in recommender systems.⁴⁷² More broadly, the equal treatment of harmful and illegal content under the DSA has been criticised by scholars.⁴⁷³

The need to take into account fundamental rights in the context of moderation activities is not only addressed by Article 14 of the DSA, but also in the provisions regarding systemic risks assessment for VLOPs and VLOSEs, as outlined in the next paragraph.

Fundamental rights and moderation activities in the systemic risks assessment for VLOPs and VLOSEs

⁴⁷¹ See *infra*: Chapter V.

⁴⁷² Frosio and Geiger (n 180) 45.

⁴⁷³ See: Aina Turillazzi et al., ‘The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications’, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 12 January 2022), 11, <https://doi.org/10.2139/ssrn.4007389>. Frosio and Geiger, ‘Taking Fundamental Rights Seriously in the Digital Services Act’s Platform Liability Regime’, 42.

The DSA provisions concerning systemic risks assessment were illustrated in the previous chapter.⁴⁷⁴ These provisions are broadly based on the recognition that major platforms, those designated as VLOPs and VLOSEs, have the capacity to generate a range of systemic risks to society through their activities. In the previous chapter, these obligations were analysed from the perspective of the risk linked to the dissemination of illegal and harmful content. Conversely, this chapter shifts focus to risks stemming from the moderation itself, such as the undue restriction of freedom of expression, freedom to receive and impart information, media pluralism, and non-discrimination.⁴⁷⁵ In essence, systemic risks may both stem from a lack of moderation and from excessive or disproportionate moderation practices. This duality is well illustrated by the risk of a ‘*negative effect on public debates*’, which may result from either under-enforcement or over-enforcement of content moderation.

Among factors potentially generating systemic risks, the DSA explicitly mentions content moderation systems and terms and conditions, as they may be discriminatory, inaccurate, or otherwise detrimental to fundamental rights and democratic dynamics.⁴⁷⁶ With regards to the mitigations measures envisaged by Article 35, they include the revision of terms and conditions, the amendment of moderation procedures, and compliance with the decisions of ODS bodies.⁴⁷⁷ More specifically, when referring to moderation procedures, the EU legislators highlights two important features: speed and quality. While the emphasis on timeliness is likely related to the prompt removal of certain type of harmful content, the focus on quality reflects the need for accuracy, fairness, and the avoidance of over-removal. In essence, the DSA requires major platforms to strike a balance between competing rights and interests in the context of moderation activities and justify

⁴⁷⁴ See *supra*, Chapter II, Section 2.4.

⁴⁷⁵ DSA, Article 34(1).

⁴⁷⁶ DSA, Article 34(2).

⁴⁷⁷ DSA, Article 35(1)(b)(c)(g).

that balance before public authorities in the context of their systemic risk assessment.⁴⁷⁸

Having analysed the provisions of the DSA aiming at regulating and bounding the moderation activities of digital intermediaries, it is now pertinent to examine the rules established by the European Media Freedom Act, and in particular its Article 18. This article may be regarded as a *lex specialis* to the DSA, as it imposes additional obligations on Very Large Online Platforms when handling content provided by media service providers. This regime closely resembles the so-called ‘*media exemption*’ proposed during the negotiations leading to the adoption of the DSA in the European Parliament, whose purpose was precisely to protect media from platforms’ moderation practices but was then abandoned due to a lack of consensus.⁴⁷⁹

2. CONTENT RESTRICTIONS TOWARDS MEDIA ENTITIES ON VLOPs: THE SPECIAL EMFA’S REGIME

The Media Freedom Act (EMFA) was adopted on 11 April 2024 by the European Parliament and the Council and has entered into force since 7 May 2024. It constitutes the first example of EU Regulation directly addressing media freedom and pluralism. Previous European regulations regarding the media sector had as main objective to strengthen the single market and facilitate the circulation of media services. The EMFA has, conversely, a broader scope, as its name suggests. In fact, media services are not here addressed merely as an economic sector, but because they ‘*provide access to a plurality of views and reliable sources of information to citizens and businesses alike, thereby fulfilling the general interest function of*

⁴⁷⁸ See *supra*: Chapter II, Section 2.4.

⁴⁷⁹ Luca Bertuzzi, ‘Media Exemption Ruled out in DSA Negotiations, but Could Return’ (*Euractiv*, 24 November 2021) <<https://www.euractiv.com/section/digital-single-market/news/media-exemption-ruled-out-in-dsa-negotiations-but-could-return/>> accessed 9 May 2025.

*‘public watchdog’ and being an indispensable factor in the process of the formation of public opinion’.*⁴⁸⁰

The legal basis used is the same as that of former regulations addressing media services, and also the same as for the DSA, namely Article 114 TFEU.⁴⁸¹ However, although the choice of this legal basis limited the potential scope of the Regulation, its objective is to ensure a minimum protection for media service providers in all Member States,⁴⁸² with a view of safeguarding fundamental rights, such as the right to receive and impart information, and democracy. In fact, strengthening media freedom was among the objectives pursued by the 2020 European Democracy Action Plan.⁴⁸³ The other two general objectives of the Plan were the promotion of free and fair elections and the fight against disinformation, both closely connected with a healthy media environment.

This Regulation has also the objective to address the digital transformation affecting the media sector. More precisely, it acknowledges how all media services (audiovisual services, radio and press) are now accessible through the internet,⁴⁸⁴ a phenomenon usually referred to as *‘convergence’*.⁴⁸⁵ Digitalisation is also seen as generating numerous market failures because of the key role in content distribution

⁴⁸⁰ EMFA, Recital 1.

⁴⁸¹ Annegret Engel, ‘Licence to Regulate: Article 114 TFEU as Choice of Legal Basis in the Digital Single Market’ in Annegret Engel, Xavier Groussot and Gunnar Thor Petursson (eds), *New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights* (Springer Nature Switzerland 2025) <https://doi.org/10.1007/978-3-031-65381-0_2> accessed 11 April 2025; Christina Etteldorf, ‘Why the Words “But” and “However” Determine the EMFA’s Legal Basis’ [2023] *Verfassungsblog* <<https://verfassungsblog.de/why-the-words-but-and-however-determine-the-emfas-legal-basis/>> accessed 11 April 2025.

⁴⁸² Roberto Mastroianni and Fabio Ferrario, *Libertà di informazione e diritto dell’Unione europea. Le nuove sfide a tutela della democrazia e del pluralismo*. (Editoriale Scientifica 2022) 10 <<https://www.libreriauniversitaria.it/liberta-informazione-diritto-unione-europea/libro/9791259764492>> accessed 13 November 2024.

⁴⁸³ European Commission, ‘Communication from the Commission to the European Parliament, the Council, the European Social and Economic Committee and the Committee of the Regions on the European Democracy Action Plan’.

⁴⁸⁴ EMFA, Recital 3.

⁴⁸⁵ Jenkins (n 105).

recently assumed by ‘*global online platforms*’, which act as ‘*gateways to media content*’.⁴⁸⁶ The first market failure regards the tendency of platforms’ business model to amplify polarising content and disinformation. The second concerns the strong competition they exercise in the advertising market, weakening media’s financial sustainability and, therefore, pluralism and diversity. Indeed, the protection of the media is also sought by the DSA, which requires VLOPs and VLOSEs to take it into consideration under systemic risks assessment.⁴⁸⁷

Following this perspective, the EMFA include several provisions aimed at strengthening the independence of legacy media *offline* (e.g., rules on ownership transparency, media mergers, editorial independence, state advertising, and the protection of journalistic sources), as well as specific provisions to protect media service providers *online*. The overarching idea underpinning the Regulation is that the role of legacy media remains crucial to reinforcing democracy and counterbalancing negative trends that have emerged in the digital landscape, such as the spread of disinformation and misinformation, acting thus as an ‘*antidote*’.⁴⁸⁸

In this section, special attention is paid to the rules governing the prerogatives of media services on digital platforms, as set out in Article 18 and 19 of the EMFA (Section 2.2). However, before delving into the analysis of these provisions, it is necessary to first examine the scope of the EMFA and, therefore, the definition of ‘media service’ (Section 2.1).

2.1. SCOPE OF THE MEDIA FREEDOM ACT: THE DEFINITION OF ‘MEDIA SERVICE’

⁴⁸⁶ EMFA, Recital (4).

⁴⁸⁷ DSA, Article 34(1)(b).

⁴⁸⁸ Natali Helberger, Max van Drunen and Ronan Fahy, ‘The Platform-Media Relationship in the European Media Freedom Act’ [2023] *Verfassungsblog* 1 <<https://verfassungsblog.de/emfa-platforms/>> accessed 13 November 2024.

The first element of the EMFA worth analysing is the definition of ‘media service’. After recalling the definition of ‘service’ set out in Article 57 TFEU,⁴⁸⁹ Article 3 states that the principal purpose of a media service consists in providing programmes or press publications to the general public under its editorial responsibility, with the purpose to inform, entertain or educate. Thus, a ‘media service provider’ is defined as a natural or legal person whose professional activity is to provide a media service and who exercises editorial responsibility for the selection of the content and the way it is organised. The definition does not depend on the distribution channel used, meaning that media operating exclusively online are subject to the same rules as traditional media, thus creating a level playing field across the internal market. Conversely, the preamble of the Regulation clarifies that the definition of a media service excludes user-generated content uploaded on online platforms, unless it constitutes a professional activity, typically carried out behind remuneration.⁴⁹⁰

On this point, it is relevant to consider the status of influencers to assess whether, in certain cases, they may qualify as providers of media services under the EMFA. In this regard, the Council has recently published conclusions on the legal status of influencers,⁴⁹¹ defined as follows:

‘Influencers’ are online content creators who post content on social media or video-sharing platforms through which they impact society, public opinion and the personal views of their audience, often showcased through their authenticity-based relationship with their audience. Influencers often have a commercial intent and engage with commercial actors through different business models for monetisation

⁴⁸⁹ Services shall be considered to be ‘services’ within the meaning of the Treaties where they are normally provided for remuneration, in so far as they are not governed by the provisions relating to freedom of movement for goods, capital and persons. ‘Services’ shall in particular include: (a) activities of an industrial character; (b) activities of a commercial character; (c) activities of craftsmen; (d) activities of the professions [...].

⁴⁹⁰ EMFA, Recital 9.

⁴⁹¹ Council of Europe, ‘Council Conclusions on Support for Influencers as Online Content Creators’ <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024XG03807>>.

purposes. Influencers can also engage in off-line activities, such as patronage, meet-and-greets and product lines.

The Council explicitly acknowledges that influencers may qualify as media service providers for the purpose of the EMFA when they meet the requirements of Article 2.⁴⁹² This means they must engage in a professional activity aimed at informing, entertaining or educating the public, while exercising editorial responsibility over their content. More broadly, given influencers' growing role in shaping public opinion online, the need to foster their accountability has emerged.⁴⁹³ If they are subject to certain obligations applicable media services, it may also be necessary to extend to them some of the protections afforded to traditional media outlets. However, when looking at the conditions set by Article 18 of the EMFA, namely the submission to a national regulatory authority or the adherence to recognised journalistic standards, the Regulation appears to intentionally privilege legacy media organisations, deemed better positioned to counteract negative dynamics in the current information system. This approach may not be the optimal solution in order to safeguard media freedom as a whole, since various forms of journalism, including non-profit and voluntary journalism, also contribute significantly to media pluralism and diversity. For instance, voluntary journalism risks being excluded from the scope of protection, as 'professionalism' under the EMFA appears to be understood primarily in terms of remuneration.⁴⁹⁴ This highlights a recurring challenge in media regulation, sometimes referred to as the '*paradox of privilege*': protecting the media requires defining who qualifies for such protection,

⁴⁹² Council of Europe (n 491) §18.

⁴⁹³ For instance, the Italian Communication Authority (AGCOM) has stated that certain obligations applicable to audiovisual services providers under the AVMS Directive (and its implementing national law) also apply to influencers (See: AGCOM, Allegato A alla delibera n. 197/25/cons, *Linee guida volte a garantire il rispetto delle disposizioni del Testo unico da parte degli influencer*).

⁴⁹⁴ Damian Tambini, 'The EU Is Taking Practical Measures to Protect Media Freedom. Now We Need Theory.' (*Centre for Media Pluralism and Freedom*, 9 May 2023) <<https://cmpf.eui.eu/the-eu-is-taking-practical-measures-to-protect-media-freedom-now-we-need-theory/>> accessed 13 November 2024.

which in turn creates space for institutional or political control over what counts as ‘media’.⁴⁹⁵

Regarding online platforms, the EU legislator has clarified that, although playing a key role in the organisation and dissemination of content, they do not typically exercise editorial responsibility over the content provided, thereby excluding them from being qualified as ‘media’.⁴⁹⁶ However, when an online platform display a section of its services over which it exercises editorial responsibility, it may, in relation to that specific service, qualify as a media service provider. This distinction also opens the door to differentiated liability regimes for platforms, particularly in relation to services like Google News.

Before turning to the provision governing the relationship between media services and major online platforms, it is worth noting that Article 3 of the EMFA enshrines the right of recipients of media services to ‘have access to a plurality of editorially independent media content’. This provision can be viewed as a specification of Article 11 of the Charter, requiring Member States and EU institutions to respect and promote media freedom and pluralism, rights that may now be directly actionable before national courts.

2.2. A ‘MEDIA PRIVILEGE’ ON VLOPS

For the purpose of this research, the most relevant provisions of the Media Freedom Act are Article 18 and 19, which specifically regulate the position of media service providers on major platforms.⁴⁹⁷ Their overarching objective is to provide

⁴⁹⁵ Tambini (n 494).

⁴⁹⁶ EMFA, Recital 11.

⁴⁹⁷ There are two other interesting provisions. First, Article 20 enshrines a ‘right to customise the media offering’, establishing that users shall have the right to easily change the configuration of any device or user interface managing access to media services in accordance with their interests. Secondly, Article 24 contains certain provisions to ensure transparency of audience measurement systems, included those employed by online platforms (See: EMFA, Recital 69). The provision is relevant because impact on the asymmetry existing between media services (as well as other commercial operators) and online platforms on advertisement.

additional safeguards to media actors against content moderation activities carried out by VLOPs.⁴⁹⁸ The underlying rationale is that VLOPs should not be permitted to supervise the activities of media outlets that adhere to established journalistic standards,⁴⁹⁹ thereby creating a form of ‘media privilege’.⁵⁰⁰

In this context, Article 18 first requires VLOPs to provide a functionality that enables recipients of their services to declare themselves as media service providers.⁵⁰¹ Alongside this declaration, the media provider must submit a set of information, including:

- a) their editorial independence from Member States and third countries;
- b) the subjection to national regulatory requirements or the adherence to a co-regulatory or self-regulatory mechanism on editorial standards widely recognised;⁵⁰²
- c) their contact details.

Once this declaration is submitted, the information must be made publicly available online, and the VLOP is required to provide dedicated contact details to ensure efficient and rapid communication with the media service provider. If a VLOP invalidates or rejects a media providers’ declaration, the provider may resort to mediation in line with Article 12 of EU Regulation No. 2019/1150 or through ODS bodies in line with Article 21 of the DSA.⁵⁰³

⁴⁹⁸ As defined by the DSA, Article 33.

⁴⁹⁹ Elda Brogi, ‘The European Media Freedom Act: Media Freedom, Freedom of Expression and Pluralism’ (Policy Department for Citizens’ Rights and Constitutional Affairs Directorate-General for Internal Policies, European Parliament 2023) PE 747.930 60 <[https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2023\)747930](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)747930)> accessed 13 November 2024.

⁵⁰⁰ Matteo Monti, ‘Why Online Public Discourse Needs a Media Privilege: In Defence of Article 18 of the EMFA’ (*Centre for Media Pluralism and Media Freedom | EMFA Observatory*, 1 November 2024) <<https://cmpf.eui.eu/in-defence-of-article-18-of-the-emfa/>> accessed 11 February 2026.

⁵⁰¹ The Commission must issue guidelines to facilitate the effective implementation of the functionality.

⁵⁰² On this point, see: EMFA, Recital 53.

⁵⁰³ EMFA, Article 18(7).

Following such self-declaration, if a VLOP intends to suspend the provision of its services towards a media entity, or to restrict the visibility of specific content, it must issue a prior notice. This obligation applies only when the restriction is based on non-compliance with the platform's terms and conditions, and not when the restriction concerns illegal content. The notice must include a statement of reasons that complies with Article 17 DSA, as well as Article 4(1) of the EU Regulation No. 2019/1150.⁵⁰⁴ Importantly, the statement of reasons must be issued *before* any enforcement action is taken, thereby granting the media service provider the opportunity to respond and present its defence in advance. Media service providers must be allowed 24 hours to respond, although a shorter time frame may apply in crisis situations requiring urgent moderation.⁵⁰⁵ This requirement marks a significant departure from Article 17 of the DSA, which only mandates a statement of reasons at the time the restriction is applied. In this perspective, Article 18 of the EMFA enhances the protection of media content on platforms. Subsequently, if the VLOP decides to proceed with the restriction of visibility, whether after receiving a reply or in its absence, it must notify the media service provider without undue delay.

Additionally, VLOPs are required to take all necessary steps to ensure that complaints submitted by media service providers are handled with priority and without undue delay. Consequently, the right of appeal is strengthened compared to the standard complaint-handling requirements applicable to 'ordinary' recipients under Article 20 DSA. Furthermore, VLOPs must publish annual transparency reports indicating the number of restrictions applied to media service providers and the grounds for those restrictions; the number of dialogues initiated under Article 18 (*infra*); and the number of rejected or invalidated declarations made by media services.⁵⁰⁶ This obligation mirrors and expands upon the transparency

⁵⁰⁴ EMFA, Article 18(4).

⁵⁰⁵ As defined by the DSA, Article 36(2). See also: EMFA, Recital 50.

⁵⁰⁶ EMFA, Article 18(8).

requirements established under Articles 15 and 24 of the DSA, introducing additional reporting duties for VLOPs specifically focused on media-related moderation.

Indeed, Article 18 grants media service providers the right to trigger a dialogue with a VLOP if they believe that repeated restrictions or suspensions have been imposed without sufficient grounds. The objective of the dialogue is to find an amicable solution. In such cases, the media service provider may also request the Board for Media Services (EBMS)⁵⁰⁷ to issue an opinion, and/or decide to notify the outcome of the dialogue to the EBMS or to the Commission. If an amicable solution is not found, the media service provider may again resort to mediation or to ODS bodies.⁵⁰⁸ In addition to this, Article 19 of the EMFA mandates the EBMS to regularly organise a structured dialogue including VLOPs, media service providers, and of civil society representatives. The dialogue is intended to: (a) discuss on the application of Article 18; (b) promote access to a plurality of independent media on VLOPs; and (c) monitor adherence to self-regulatory frameworks aimed at countering harmful content, disinformation, and foreign interference. The EBMS must report the outcomes of these dialogues to the Commission and, where possible, make them publicly available. This provision appears to build upon the experience of the Code of Practice on Disinformation,⁵⁰⁹ while introducing a notable innovation, namely the formal involvement of media service providers.

Despite its noble purpose, the special regime established by Article 18 of the EMFA for media service providers on major online platforms presents a number of limitations. Firstly, it applies only to media service providers as defined by Article

⁵⁰⁷ The European Board for Media Services is established by Article 8 EMFA and it replaces and succeeds the European Regulators Group for Audiovisual Media Services (ERGA) established by Article 30b of Directive 2010/13/EU. It is composed of representatives of national regulatory authorities or bodies.

⁵⁰⁸ EMFA, Article 18(7).

⁵⁰⁹ Brogi (n 499) 63.

2 of the Regulation. Second, among those, only a limited subset is likely to be eligible for the protection in question, since they also must meet the additional requirements laid out in Article 18(1). In particular, they must demonstrate their editorial independence, a vague and controversial concept,⁵¹⁰ that could grant online platforms significant discretion in determining eligibility.⁵¹¹ However, this uncertainty has been partially mitigated by the adoption of guidelines by the European Commission, which establish procedures for consulting relevant regulatory authorities and involving civil society organisations, including fact-checkers, in the review of declarations.⁵¹²

In any event, to qualify as media they must be subject to a national media regulator or abide to established international journalistic standards, a feat that mainly applies to traditional media entities. Third, it is unclear why the Regulation restricts its scope to Very Large Online Platforms, without extending equivalent obligations to Very Large Online Search Engines. Although content restrictions by search engines may be less frequent, this exclusion appears inconsistent, especially when considering that, under the DSA, VLOPs and VLOSEs are generally subject to equal obligations. Additionally, the prior notice mechanism applies only to restrictions based on the violation of a platform's terms and condition, not when the content is deemed illegal. More specifically, that this mechanism does not apply to restrictions adopted under Articles 28, 34 and 35 of the DSA, Article 28b of the AVMS Directive, or in any case where content is deemed illegal under EU law. These exceptions significantly narrow the scope of the additional protection granted by the EMFA. Indeed, no prior notice is required not only when a national authority

⁵¹⁰ Joan Barata, 'Protecting Media Content on Social Media Platforms' [2022] Verfassungsblog 3 <<https://verfassungsblog.de/emfa-dsa/>> accessed 13 November 2024.

⁵¹¹ Barata (n 510) 3.

⁵¹² European Commission, 'Commission Guidelines on the Implementation of the Declaration Functionality for Media Service Providers Pursuant to Article 18 (1) of Regulation (EU) 2024/1083 (European Media Freedom Act)' <<https://ec.europa.eu/newsroom/dae/redirection/document/124304>>.

had determined the content to be illegal, but also when the platform itself deems the content illegal, or when it classifies the content as ‘harmful’ under the AVMS Directive,⁵¹³ or when its restriction is part of broader systemic risk mitigation measures under the DSA. In all these cases, the general safeguards provided by the DSA remain applicable, and media service providers appear to retain the benefit of priority treatment in the handling of their complaints.

Moreover, scholars have criticised the EMFA’s reliance on dialogue and transparency to correct the structural power asymmetry between media actors and online platforms, considering it an overly soft approach.⁵¹⁴ In particular, the provisions on enforcement have been described as vaguely drafted, adding a worrying dimension of negotiability to fundamental rights and media protection.⁵¹⁵ This criticism echoes similar concerns raised in the context of the DSA, especially with regard to the requirement for platforms to balance fundamental rights against other interests when moderating content.⁵¹⁶ Nevertheless, it is possible that the introduction of structured dialogue may serve as a first step toward more robust regulatory obligations in the future. Lastly, and in contrast with the DSA, the EMFA does not explicitly confer on media service providers subject to content restrictions the right to seek redress before national courts; nevertheless, such a possibility cannot be regarded as excluded.

CONCLUDING REMARKS

⁵¹³ As already mentioned above, Article 28b require Member States to ensure that VSP providers protect (a) minors from communications which may negatively affect their physical, mental or moral development; (b) the general public from communications containing incitement to violence or hatred; (c) the general public from communications containing content which constitutes a criminal offence under Union law, including provocation to terrorism, child pornography, racism and xenophobia.

⁵¹⁴ Helberger, van Drunen and Fahy (n 488) 3.

⁵¹⁵ In this regard, some authors claimed: *«the rule of law and procedural rights are replaced by a “meaningful and effective dialogue”. In case an interference with fundamental rights is found, an authoritative declaration of its impermissibility is turned into “finding an amicable solution”»* (Helberger, van Drunen and Fahy (n 488) 5.).

⁵¹⁶ See *supra*: Section 1.3.

Moderation activities by digital platforms are fully legitimised under the new EU regulatory framework, and as a consequence, so is their broader role in filtering content. As discussed in the previous chapter, content removal is sometimes mandatory, particularly when an intermediary becomes aware of illegal content through a notification submitted by public authorities or users. Moreover, platforms can also engage in spontaneous moderation of illegal and harmful content, as defined in their terms and conditions. While the EU's Good Samaritan clause (Article 7 of the DSA) explicitly safeguards the voluntary removal of *illegal* content, the DSA generally treats the moderation of merely *harmful* content on equal terms.

However, spontaneous moderation is subject to two key types of limitations. The first limitation consists of a general (albeit vague) obligation to respect fundamental rights, which carries greater weight in the context of systemic risks obligations.⁵¹⁷ The second limitation is procedural, consisting of a detailed set of due process safeguards, such as the obligation to provide a statement of reasons and access to redress mechanisms,⁵¹⁸ along with multiple transparency requirements.⁵¹⁹ While the obligation to respect fundamental rights can influence the *content* of moderation decisions, it remains imprecise and open-ended. In contrast, procedural rules have been elaborated in far greater detail, making the DSA's most substantial contribution the insertion of rule-of-law principles into the content moderation process. Ultimately, the regulatory framework remains largely silent on the unilateral rule-making power of platforms, i.e. their authority to define what qualifies as 'harmful' speech within their own terms of service. This greater emphasis on procedural safeguards has led scholars to characterise the DSA as adopting a 'procedure before substance' approach.⁵²⁰

⁵¹⁷ See *supra*: Section 1.3.

⁵¹⁸ See: Section 1.2

⁵¹⁹ See: Section 1.1.

⁵²⁰ Ortolani (n 20) 154.

Broadly speaking, these rules enshrine platforms' power over information flows, effectively accepting a model of private governance over the Internet, including from a fundamental rights perspective.⁵²¹ However, the overall power of platforms is partially rebalanced through a series of obligations that introduce greater pluralism into the governance of the digital public sphere. External actors are increasingly empowered to participate in moderation decisions: public authorities, users and trusted flaggers can trigger content restrictions;⁵²² media service providers benefit from specific prerogatives under the EMFA;⁵²³ and out-of-court dispute settlement bodies offer users an independent review of moderation decisions.⁵²⁴ Moreover, all these rules on content moderation authorise competent public authorities to scrutinise platforms' moderation activities, ensuring that they align with the obligations set out under the DSA. Notably, given that online platforms were already enforcing restrictions on harmful content via their terms of service, the introduction of transparency and procedural safeguards marks a significant advancement for users' rights. These boundaries, taken together, can contribute to aligning moderation decisions more closely with the public interest, reconciling private governance with social and democratic accountability. However, the deeper question, whether private actors should retain such broad discretion over what constitutes acceptable speech, remains only partially addressed.

This question also extends to other digital actors, such as generative AI systems. Even if they act as distributors of third-party information, not all their functionalities fall within the category of intermediary activities and are therefore partially excluded from the scope of the DSA. Even though the nature of their services is less suitable for procedural rules on content restrictions, their choices to

⁵²¹ Cauffman and Goanta (n 464) 768. Goanta and Ortolani (n 465); Frosio (n 465).

⁵²² See: Chapter II, Section 2.3.

⁵²³ See: Section 2.2.

⁵²⁴ Albeit without binding authority. See: Section 1.2.

exclude certain perspectives and voices from the public debate remain concerning and currently escapes public scrutiny.

IV. PRIORITISATION, RANKING, AND RECOMMENDER SYSTEMS

The prioritisation, ranking and recommendation of content represent the second major way in which platforms shape information transmission and set the rules governing its flow. Major platforms systematically sort and prioritise information according to various criteria that do not reflect the chronological order of upload. While the terms *prioritisation*, *ranking* and *recommendation* refer to slightly different operations on content, they all concern the question of which content reaches a single user, and in which sequence. For the sake of simplicity, all these practices are referred here as *recommender systems*, a notion which underlines the personalised nature of content curation in the digital environment.

Unlike moderation, recommender systems do not remove content from the platform but significantly influence its visibility and reach: they do not determine who can speak but rather who gets heard.⁵²⁵ As such, they are more closely connected to issues of media pluralism and opinion power than to freedom of expression: they mirror the agenda-setting power traditionally held by the media, meaning the ability to shape public debate priorities by choosing which news deserve priority coverage.⁵²⁶ From this perspective, these practices have sometimes been compared to editorial curation.⁵²⁷

In the modern era, alongside the development of the media, visibility has become a crucial factor in shaping power dynamics within the public sphere.⁵²⁸ However, the importance of visibility has been exacerbated with the advent of digital platforms,⁵²⁹ as shown, for instance, by studies on the exponential drop in click

⁵²⁵ Wu, 'Is the First Amendment Obsolete?' (n 114).

⁵²⁶ Napoli (n 7) 54.

⁵²⁷ See *supra*: Chapter II, Section 1.2.

⁵²⁸ John Thompson, 'The New Visibility' (2005) 22 *Theory, Culture & Society* 31. Gillespie (n 60) 171.

⁵²⁹ Wu, 'Is the First Amendment Obsolete?' (n 114) 556.

rates depending on the order in which results appear on Google.⁵³⁰ Scholars have identified the overwhelming amount of information characterising the digital society as the main reason for this situation. This abundance of information has been referred to in various ways, including ‘*information flood*’⁵³¹ and ‘*cheap speech*’;⁵³² and it has been consistently illustrated how this implies a corresponding scarcity of human attention.⁵³³ Consequently, in the information-rich age, one very effective mean of controlling speech is targeting the bottleneck of attention, instead of speech itself.⁵³⁴

The early internet was already characterized by an abundance of information. Open access and disintermediation led to a proliferation of blogs and websites, creating a chaotic navigating experience where relevant information was often difficult to find.⁵³⁵ This situation paved the way for the rise of some major platforms offering content curation services to users.⁵³⁶

In digital platforms, content curation is essentially determined by algorithms, whose functioning has long been opaque, therefore referred to as ‘black boxes’.⁵³⁷ It is, however, generally understood that these algorithms sort information based on three main parameters, often combined: (1) alignment with user preferences, (2)

⁵³⁰ Philip Petrescu, ‘Google Organic Click-Through Rates in 2014’ (*Moz*, 1 October 2014) <<https://moz.com/blog/google-organic-click-through-rates-in-2014>> accessed 7 January 2025.

⁵³¹ James Gleick, *The Information: A History, a Theory, a Flood* (Knopf Doubleday Publishing Group 2011).

⁵³² Eugene Volokh, ‘Cheap Speech and What It Will Do’ [1995] *Yale Law Journal* <<https://openyls.law.yale.edu/handle/20.500.13051/8884>> accessed 25 February 2025.

⁵³³ Cited in: Wu, ‘Is the First Amendment Obsolete?’ (n 114) 554.

⁵³⁴ Wu, ‘Is the First Amendment Obsolete?’ (n 114) 554. This is why flooding campaigns of bots and disinformation can be very effective. For example the Chinese government not only suppresses speech, but creates distraction campaigns (Wu, ‘Is the First Amendment Obsolete?’ (n 114) 557.). the ‘flooding’ technique has also been promoted by Steve Bannon (Philip M Napoli, ‘In Pursuit of Ignorance: The Institutional Assault on Disinformation and Hate Speech Research’ (2025) 41 *The Information Society* 1, 3 <<https://doi.org/10.1080/01972243.2024.2419105>> accessed 18 June 2025.)

⁵³⁵ Napoli (n 7) 24.

⁵³⁶ Gillespie (n 60) 13.

⁵³⁷ Napoli (n 7) 53; Pasquale (n 152).

popularity, and (3) paid advertising. This interplay of parameters lies at the heart of the challenges related to recommender systems, as further discussed below.

Unlike today, content recommendation was not a central feature for all platforms when they first emerged. For instance, Facebook presented news in a reverse chronological order from 2006 to 2009, and Twitter and Instagram incorporated algorithmic filtering only in 2016, after respectively 10 and 6 years of activity.⁵³⁸ Until 2009, Google presented content based on relevance but without personalised results.⁵³⁹ These changes were mainly linked to the development of these platforms' business model, based on the need to maximise user engagement in order to sell ads.⁵⁴⁰ This model is well described by the concept of 'attention economy', combined with the dynamics of 'surveillance capitalism'.⁵⁴¹

The mechanisms of 'attention economy' are shared by all advertisement-driven businesses.⁵⁴² As such, they are also typically present in traditional media outlets, because the more time users spend on a single outlet, the more the advertisement on that outlet is valuable.⁵⁴³ This means that, to maximise profit, the content transmitted through these outlets must be as engaging as possible. Consequently, choices about media content have traditionally been shaped by a combination of what is believed to be relevant and what the audience find appealing (i.e., what people want).⁵⁴⁴ In the platform economy, these mechanisms are combined with the extensive use of personal data, enabling an incomparably more precise

⁵³⁸ Napoli (n 7) 34.

⁵³⁹ Pariser (n 135).

⁵⁴⁰ Napoli (n 7) 34.

⁵⁴¹ Zuboff (n 32). See also *supra*: Chapter I, Section 1.2.

⁵⁴² Wu, 'Is the First Amendment Obsolete?' (n 114) 555.

⁵⁴³ As already mentioned above (Chapter I, Section 1.2.), scholars have conceptualised attention as a product that users provide to platforms in exchange for their services, and which platforms then sell to the highest bidder in the downstream advertising market (Newman (n 26)).

⁵⁴⁴ Napoli (n 7) 56.

determination of ‘what users want’ and giving rise to a surveillance-based advertising model.⁵⁴⁵

In fact, the enormous profits generated by tech giants are notoriously driven by the monetization of user data, as its extraction is crucial for attracting advertisers, given that the more precisely an ad is targeted, the more efficient it becomes. Social media platforms are a gold mine of personal data due to the vast amount of information voluntarily shared by users.⁵⁴⁶ However, data is also ‘*extracted*’, i.e. combined and inferred from any online behaviour, including visited websites, purchases, metadata – resulting in the largest commercial collection of personal data in history.⁵⁴⁷ As UN Secretary Antonio Guterres once warned: ‘*Our data is being bought and sold to influence behaviour*’.⁵⁴⁸

Since digital platforms depend on users spending as much time as possible on their services to maximise profits, their recommender systems are designed to present engaging content. In this context, data collection functions both as the means and the end of keeping users attached to these platforms, as vast datasets enable digital services to determine precisely which content can capture users’ attention. This analytical framework helps to explain the rationale behind the three parameters used in recommender systems: while advertised content represents the source of profit, popular and personalised content serve as the means to sustain user engagement.

⁵⁴⁵ Sebastian Becker and Jan Penfrat, ‘The DSA Fails to Reign in the Most Harmful Digital Platform Businesses – But It Is Still Useful’ in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023) 56.

⁵⁴⁶ Napoli (n 7) 39.

⁵⁴⁷ Personalised content is typically displayed based on an individual user’s preferences or those of others with similar characteristics, such as age, gender, geographic location, political views, and beliefs as described by Napoli (n 7) 35. See also: Becker and Penfrat (n 545) 56.

⁵⁴⁸ António Guterres, ‘Social Media Platforms Based on a Business Model That Monetizes Anger & Negativity Are Causing Untold Damage to Societies. Hate Speech & Misinformation Are Proliferating. Our Data Is Being Bought & Sold to Influence Behaviour. We Need Regulatory Frameworks to Change This.’ <<https://x.com/antonioguterres/status/1574111500201074688>> accessed 29 October 2025.

The attention economy based on surveillance capitalism presents multiple drawbacks for both individual and society. First, it incentivises ‘addictive design’ of recommender systems,⁵⁴⁹ while also rendering users highly vulnerable to manipulation. Second, as extreme content tends to attract more attention than moderate perspectives, platforms algorithms have been found to amplify such material to maximise engagement.⁵⁵⁰ Third, according to some scholars, it would create ‘echo chambers’, also referred to as ‘filter bubbles’ or ‘information cocoons’,⁵⁵¹ where users are primarily exposed to a highly tailored package of information designed to match with their preexisting interests and beliefs.⁵⁵² The aspiration to give everyone their tailored news outlet has been also confirmed by Mark Zuckerberg himself, when stating that: ‘*Our goal is to build the perfect personalized newspaper for every person in the world*’.⁵⁵³ However, such mechanisms these mechanisms risk entrenching users’ existing views, leading to a fragmentation and polarisation of the society.⁵⁵⁴ Additional polarisation would occur when extreme content is prioritised, meaning that ‘*everyone sees exactly the information that personally aggravates them*’.⁵⁵⁵ This self-reinforcing exposure dynamic, where recommender systems gradually lead users toward increasingly radical content is often referred to as the ‘*rabbit hole*’ effect.⁵⁵⁶

⁵⁴⁹ European Parliament, ‘New EU Rules Needed to Address Digital Addiction’ (12 December 2023) <<https://www.europarl.europa.eu/news/en/press-room/20231208IPR15767/new-eu-rules-needed-to-address-digital-addiction>> accessed 29 October 2025.

⁵⁵⁰ Murthy (n 134). See also *supra*: Chapter II, Section 1.2.

⁵⁵¹ Pariser (n 135); Sunstein (n 135).

⁵⁵² Wu, ‘Is the First Amendment Obsolete?’ (n 114) 555.

⁵⁵³ Moore (n 7) 32.

⁵⁵⁴ Habermas (n 2). Arguably, such fragmentation already existed when the TV started to include different channels (Wu, *The Master Switch* (n 5) 213.), but the increased technical capacity for personalisation on digital platforms exacerbates this situation.

⁵⁵⁵ Alexandra Geese, ‘Why the DSA Could Save Us From the Rise of Authoritarian Regimes’ in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023) 71.

⁵⁵⁶ Kaitlin Woolley and Marissa A Sharif, ‘Down a Rabbit Hole: How Prior Media Consumption Shapes Subsequent Media Consumption’ (2022) 59 *Journal of Marketing Research* 453 <<https://doi.org/10.1177/00222437211055403>> accessed 29 October 2025.

Further concerns arise from targeted advertising, as profit-driven entities and malicious actors can exploit personal data for manipulation. Manipulation can also serve political motives, adding another layer of concern for fundamental rights and the functioning of democratic processes. The Cambridge Analytica scandal is a prime example in this regard, also highlighting the alarming intersection of recommender systems, data exploitation, and their impact on public opinion.⁵⁵⁷

These concerns have been taken into account by the EU lawmakers when drafting recent regulations on digital services. As a result, several provisions now govern data collection, online advertising, and recommender systems. This chapter analyses three key regulatory frameworks in relation to their approach to recommender systems: the Digital Services Act (Section 1), the Digital Markets Act (Section 2), and the Regulation on Transparency and Targeting of Political Advertising (Section 3). To better understand the impact of these provisions on recommender systems, this chapter will, where possible, provide general information on their implementation. However, given the rapidly evolving nature of both the regulatory landscape and platform policies, these insights may soon become outdated.

Since recommender systems are machine-learning algorithmic systems, the AI Act is also, in principle, applicable to them.⁵⁵⁸ However, this Regulation does not appear to have been primarily designed to govern content curation algorithms within online platforms. The transparency obligation imposed on providers of AI systems that interact directly with natural persons seems mostly relevant for chatbots,⁵⁵⁹ while the systemic risk assessment provisions add little when the provider is already designated as a VLOP or VLOSE under the DSA.⁵⁶⁰ It should also be noted that the AI Act prohibits AI systems that deploy *subliminal* techniques intended to

⁵⁵⁷ See *supra*: Chapter I, Section 2.1.

⁵⁵⁸ AI Act, Article 3.

⁵⁵⁹ AI Act, Article 50(1).

⁵⁶⁰ AI Act, Article 55.

manipulate a person's behaviour by *impairing their ability to make an informed decision* and causing therefore significant *harm*; as well as those *exploiting vulnerabilities* linked to age, disability or a social-economic situation with the objective of *distorting the person's behaviour* and thereby causing significant *harm*.⁵⁶¹ Given the manipulative nature of recommender systems, one may wonder whether these prohibitions could apply in this context. However, no official guidance or enforcement precedent has yet clarified this point.

1. THE DSA REGULATING RECOMMENDER SYSTEMS

The Digital Services Act recognises, in its preamble, that the ranking of information is a fundamental aspect of platforms' activities and that it has a significant impact on users' ability to encounter information online, as well as contributing to the amplification of certain content.⁵⁶² To this regard, the DSA emphasises the need for users to be adequately informed about how recommender systems influence the reception of information. This means that one of the main purposes of the DSA regarding recommender systems is to address the information asymmetry traditionally existing between platforms and the public society concerning the functioning of recommender algorithms.⁵⁶³ Enhanced transparency is to be achieved through a combination of measures, including general transparency obligations toward the public (analysed in Section 1.1), together with external oversight obligations. The latter include requirements for VLOPs and VLOSEs to undergo independent audits at least once a year (Article 37 DSA) and to provide vetted researchers with access to their data (Article 40 DSA).⁵⁶⁴

Beyond transparency, the DSA also seeks to limit the most high-risk recommender systems. To this end, it imposes several restrictions on the use of data for targeted advertising, particularly when based on sensitive data and addressing minors

⁵⁶¹ AI Act, Article 5(1), (a), (b).

⁵⁶² DSA, Recital 70.

⁵⁶³ Geese (n 555) 69.

⁵⁶⁴ See *infra*: Chapter V.

(Section 1.2), and it requires VLOPs and VLOSEs to assess and mitigate the systemic risks that may arise from their algorithms and recommender systems (Section 1.3).

As a preliminary note, it is important to clarify the scope of the provisions analysed in the present section. In line with the structure of escalating obligations adopted by the DSA,⁵⁶⁵ these provisions apply exclusively to online platforms and, in some cases, only to VLOPs and VLOSEs. Therefore, other types of digital intermediaries and hosting services are not addressed. This distinction is justified by the fact that intermediaries other than platforms primarily facilitate one-to-one communications: since they do not engage in communication to the public,⁵⁶⁶ their reliance on recommender systems is expected to be minimal.

1.1. TRANSPARENCY OBLIGATIONS ON RECOMMENDER SYSTEM: A RIGHT TO EXPLANATION?

The DSA includes a wide range of transparency obligations, which vary depending on the type of intermediary and the nature of the service provided. This section first examines the transparency obligations for recommender systems set out in Article 27, and then addresses those specifically related to advertising, as established in Article 26.

General transparency obligations for recommender systems

The first transparency requirement concerning recommender systems is established by Article 27 of the DSA, which obliges online platform to explain in their terms and conditions – *in plain and intelligible language* – the main parameters used in their recommender systems. The purpose of this obligation is to enable users to understand why certain content is recommended to them.⁵⁶⁷ This explanation must

⁵⁶⁵ See *supra*: Chapter II, Section 2.1.

⁵⁶⁶ See the definition of online platforms according to the DSA (*Supra*, Chapter I, Section 2.1.)

⁵⁶⁷ DSA, Article 26(1).

include the most important criteria used for recommending content, with the indication of their respective importance.⁵⁶⁸

Moreover, the platform must inform the recipients about any option *to modify or influence* those main parameters. If these options are available; platforms should provide a functionality that allows the recipients to select and to modify at any time their preferred option.⁵⁶⁹ This functionality must be easily accessible on the interface where the information is prioritised.⁵⁷⁰ This provision is strengthened for VLOPs and VLOSEs, as Article 38 mandates them to provide for an option not based on profiling (*infra*).

Scholars have examined how Meta and TikTok have implemented Article 27 of the DSA.⁵⁷¹ Meta, for instance, has introduced explanations about the signals that influence recommendations, helping users understand how their behaviour and interactions with the platform affect the content recommended to them. These explanations vary depending on the different outputs and features offered by Facebook and Instagram (e.g., Reels, Stories, Explore). TikTok, on the other hand, provides a general overview of the parameters influencing its recommender systems.⁵⁷²

However, the same scholars have observed that the control granted to users over these systems remains limited.⁵⁷³ Importantly, while the DSA mandates transparency on how user behaviour influences content recommendation, an obligation to provide users with options to modify the parameters used by

⁵⁶⁸ DSA, Article 26(2).

⁵⁶⁹ DSA, Article 26(3).

⁵⁷⁰ DSA, Article 26(3).

⁵⁷¹ Urbano Reviglio and Matteo Fabbri, 'The Regulation of Recommender Systems Under the DSA: A Transition from Default to Multiple and Dynamic Controls?' (*DSA Observatory*, 22 November 2024) <<https://dsa-observatory.eu/2024/11/22/the-regulation-of-recommender-systems-under-the-dsa-a-transition-from-default-to-multiple-and-dynamic-controls/>> accessed 13 December 2024.

⁵⁷² TikTok, 'How TikTok Recommends Content' (*tiktok.com*) <<https://support.tiktok.com/en/using-tiktok/exploring-videos/how-tiktok-recommends-content>> accessed 13 October 2025.

⁵⁷³ Reviglio and Fabbri (n 571) 3.

recommender systems does not result from the legal text. For example, on Meta's platforms, users can choose from a narrow list of reasons to indicate why they dislike a particular piece of content or specify hashtags they want to filter out of their feeds – a feature also implemented on TikTok.⁵⁷⁴ In this respect, platforms appear to have adopted a rather minimalist interpretation of Article 27, viewing it as not requiring the creation of new control options but merely ensuring accessibility where they already exist.⁵⁷⁵ An exception is represented by the introduction of a '*Refresh*' option on TikTok, allowing users to reset their recommendation as if they were new to the platform;⁵⁷⁶ a function recently added on Instagram as well.⁵⁷⁷ However, despite the importance of this option, it represents more an all-or-nothing approach rather than one that truly gives users control over specific parameters.

Moreover, wider control over recommendations would require not only filtering options to *exclude* certain content but also mechanisms to *include* it, allowing users to positively shape their results. Taking Instagram as an example, there are some minor available options to this regard.⁵⁷⁸ For instance, users can adjust the amount of sensitive⁵⁷⁹ and political⁵⁸⁰ content recommended to them from users they don't

⁵⁷⁴ Reviglio and Fabbri (n 571) 3.

⁵⁷⁵ Reviglio and Fabbri (n 571) 6.

⁵⁷⁶ TikTok, 'An Update on Fulfilling Our Commitments under the Digital Services Act' (*Newsroom | TikTok*, 16 August 2019) <<https://newsroom.tiktok.com/en-eu/fulfilling-commitments-dsa-update>> accessed 7 February 2025.

⁵⁷⁷ Instagram, 'New on Instagram: How to Reset Your Content Suggestions' (*Instagram*, 19 November 2024) <<https://about.instagram.com/blog/announcements/reset-instagram-content-suggestions>> accessed 25 February 2025.

⁵⁷⁸ Broad information about content preferences can be found here: Instagram, 'Control Your Instagram Feed' (*Instagram Blog*, 30 August 2022) <<https://about.instagram.com/blog/tips-and-tricks/control-your-instagram-feed>> accessed 25 February 2025.

⁵⁷⁹ Instagram, 'Updates to the Sensitive Content Control' (*Instagram Blog*, 6 June 2022) <<https://about.instagram.com/blog/announcements/updates-to-the-sensitive-content-control>> accessed 25 February 2025.

⁵⁸⁰ Instagram, 'Update on Political Content on Instagram and Threads' (*Instagram*, 9 February 2024) <<https://about.instagram.com/blog/announcements/continuing-our-approach-to-political-content-on-instagram-and-threads>> accessed 25 February 2025.

follow, choosing between ‘less’, ‘standard’, and ‘more’.⁵⁸¹ In addition, users are sometimes allowed to indicate whether they are interested in a specific piece of recommended content. However, this ‘interested’ option is not available for all content, and its impact on recommendations remains unclear.

More broadly, it seems like users on both platforms can only influence how content is displayed but cannot remove the original parameters that led to its recommendation. In other words, they can only modify the outputs, not the inputs. A different approach could provide users with the choice about which data feeds personalisation, e.g. their profile data or behavioural signals. This would also help users to understand the recommender system logic, allowing them to opt-out from certain types of profiling that may not align with the user’s actual or consciously expressed preferences.⁵⁸²

Transparency obligations for online advertisement

In parallel, Article 26 of the DSA introduces a series of transparency obligations regarding online advertisement. First and foremost, commercial communications must be clearly labelled as such, ensuring a distinction between advertisement and other recommended content. Second, users must have access to information about the source of the advertisement and the reason it is recommended to them. Indeed, the preamble states that users must be informed about the main parameters used to determine why a specific advertisement is presented to them, including a *meaningful explanation of the logic* behind such recommendations, particularly when they rely on profiling.⁵⁸³ Moreover, Article 39 strengthens advertising transparency for VLOPs and VLOSEs by requiring them to maintain a publicly accessible database containing key information about every advertisement displayed for a period of one year. The information to be disclosed includes the

⁵⁸¹ The ‘more’ option is excluded for minors regarding sensitive content.

⁵⁸² Reviglio and Fabbri (n 571) 8.

⁵⁸³ DSA, Recital 68.

advertised product, the advertiser, the period during which the advertisement was displayed, the targeting parameters used, and the number of users reached.⁵⁸⁴

The legality of the obligation to make an advertisement repository publicly available has been contested by certain designated VLOPs. In particular, Amazon, when challenging its designation as VLOP,⁵⁸⁵ argued that this provision infringes its fundamental rights to privacy and its freedom to conduct a business, essentially because it entails the disclosure of confidential information to competitors. While the Court has not yet ruled the substance of the case, it rejected Amazon's request for interim measures,⁵⁸⁶ holding that postponing the DSA's objective of enhancing transparency and accountability for major platforms could pose significant risks.⁵⁸⁷ Although not conclusive, this decision has been regarded as an indication that the Court is likely to attach significant weight to the public interest pursued by the DSA and to uphold its data-sharing and transparency provisions.⁵⁸⁸

Regarding the actual implementation of advertising transparency, it is useful to examine how Article 26 has been operationalised on Instagram, a popular social media platform also designated as VLOP. In the Instagram feed, advertised content is labelled as '*Sponsored*' beneath the name of the account. Users can access additional information directly from the advertised content by selecting the '*Why you're seeing this ad?*' option (Appendix, Figure 2). This feature discloses the targeting parameters used for recommending the advertisement, which are divided

⁵⁸⁴ DSA, Article 39(1).

⁵⁸⁵ CJEU, Case T-367/23, *Amazon Services Europe v Commission*, action brought on 5 July 2023.

⁵⁸⁶ Amazon also required the suspension of Article 38 of the DSA, as further discussed below.

⁵⁸⁷ *Amazon Services Europe Sàrl v European Commission* Order of the President of the General Court of 27 September 2023, Court of Justice of the European Union ECLI:EU:T:2023:589, Case T-367/23 R.

⁵⁸⁸ Beatriz Botero Arcila, 'An Early Win for the Transparency Measures of the DSA. A Comment on *Amazon Services v. European Commission* (C-638/23)' (*DSA Observatory*, 2 May 2024) <<https://dsa-observatory.eu/2024/05/02/an-early-win-for-the-transparency-measures-of-the-dsa-a-comment-on-amazon-services-v-european-commission-c-638-23/>> accessed 3 February 2025.

into two categories (Appendix, Figure 3).⁵⁸⁹ The first category includes parameters selected by the advertiser, who may choose to target users based on factors such as ‘*an age between 18 and 45*’, ‘*a primary location in Italy*’, or gender (Appendix, Figure 4). The second category includes parameters linked to the individual user’s activity, reflecting personalised advertising based on profiling techniques. In this case, the advertisement is deemed relevant to the targeted user based on inferences drawn from previous interactions on the platform or on other platforms. For example, in the case of an advertisement from a fashion company, this category included parameters such as ‘*you interacted with ads about fashion and style, clothing and travel*’, but also ‘*about pets, relationships and software and apps*’, including interactions on Facebook Marketplace (Appendix, Figure 5). When examining the operationalisation of these transparency requirements, the overall picture appears rather unsatisfactory. Indeed, the displayed explanations appear confusing and fail to provide any meaningful insight. Not only are the mentioned parameter exceedingly broad, but the lack of reference to specific actions makes it unclear how these interests are determined, while the connection between certain topics – such as pets and fashion – is not immediately evident.

When accessing this feature, users can also access Instagram’s parent company (Meta) advertisement database, where they can view all ads from the same source over the past year, even if they are no longer active. By clicking on an individual advertisement, users can see who paid for it and on whose behalf, as well as the approximate number of impressions it received. Additionally, the Meta advertisement database can be accessed directly via the web and includes ads across all Meta platforms. The database is accessible through a search function with filters by country and theme, including issues, elections, or politics; housing; employment; financial products and services. For advertisements categorized under ‘*Issues*,

⁵⁸⁹ They are divided into two categories only if the user has selected the ‘more personalised’ version of the platform (see the following paragraph: “Right to an option of recommender systems not based on profiling”). Otherwise, as ads are not based on profiling, only the first category appears.

elections, or politics’ users can immediately see the estimated audience size and the approximate amount spent, and it is possible to rank results based on the number of impressions received.⁵⁹⁰ These additional information are connected to the requirements set by the Regulation on Political Advertisement, as further discussed below (Section 3.3).

Other than imposing obligations on the transparency of recommender systems, the DSA also imposes some substantial limitations on targeting practices, especially when performed through extensive profiling activities.

1.2. RESTRICTIONS ON TARGETED RECOMMENDATIONS

As mentioned in the introduction of this Section, the DSA also addresses certain content microtargeting practices that are considered particularly dangerous. In this regard, for online intermediaries classified as platforms, the DSA introduces some restrictions on recommender systems. These provisions are largely based on the GDPR, including several references to its rules and definitions.

Restrictions on profiling practices for the purposes of online ads

The DSA includes two prohibitions on profiling for the purpose of online advertisement, both of which will be analysed in this paragraph. The first, outlined in Article 26, focuses on ‘sensitive’ data, while the second, Article 28, concerns advertising targeting minors.

More precisely, Article 26, in its final paragraph, prohibits online platform from presenting advertisements to recipients based on profiling that uses the special categories of data defined by Article 9 of the GDPR. Profiling is, in its turn, defined by Article 4(4) of the GDPR as:

any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular

⁵⁹⁰ These findings are based on research conducted on Meta platforms by the author on February 6, 2025, but the situation may evolve rapidly.

to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Essentially, profiling involves using a set of personal data about an individual or a group of people to generate new insights, meaning inferred knowledge or hypotheses about a person's behaviour, such as their preferences, personality, or health conditions.⁵⁹¹ It is the process of deriving new knowledge based on previous data – a cognitive function traditionally performed by the human brain, but now increasingly carried out by machine learning algorithms.⁵⁹²

The prohibition of profiling only relates to the special categories of data listed in Article 9(1) of the GDPR, which are particularly sensitive data. This list include data:

revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The list provided by the GDPR aims to prohibit the processing of these categories of data. However, the GDPR prohibition includes significant exceptions: most notably, the ability to process 'sensitive data' with the explicit and specific consent of the data subject. In contrast, under the DSA, profiling using personal data for targeted advertising is entirely prohibited. However, the DSA prohibits only *profiling*, not the mere *processing* of 'sensitive' data. Consequently, this data can still be collected on platforms if the requirements set by Article 9 GDPR are met, but it may only be used for recommending non-advertised content.

⁵⁹¹ Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (Social Science Research Network, 23 May 2017) 32 <<https://papers.ssrn.com/abstract=2972855>> accessed 13 November 2024.

⁵⁹² Edwards and Veale (n 591) 32.

The decision to entirely prohibit the targeting of advertising based on profiling involving sensitive data, regardless of user consent, represents a highly reasonable approach on multiple levels, particularly in light of the need for robust privacy protection online and the largely fictitious nature of consent in the digital environment.⁵⁹³ Moreover, by acknowledging that targeting users with advertisements tailored to their interests and potentially exploiting their vulnerabilities can have serious negative effects, the DSA addresses not only individual but also societal harms. Manipulative techniques can damage entire groups and amplify collective risks, for example by fuelling disinformation campaigns or enabling discriminatory practices.⁵⁹⁴ Unlike the GDPR, which primarily focuses on the protection of individual rights, and therefore relies on consent, this provision appropriately considers data protection as a tool to safeguard society as a whole from manipulation.⁵⁹⁵

However, this provisions also presents some weaknesses. First, manipulation is not only possible through the use of particularly sensitive data but can also be carried out by exploiting large-scale datasets, since the sheer volume of available data enables a very precise identification of patterns and correlations. As such, this provision may be seen as a compromise between a total ban on using any personal data for targeting advertising (as mandated by Article 28 for minors) and the previous situation, where any data processing was permitted.⁵⁹⁶ Indeed, EU lawmakers ultimately chose to limit the scope of the restrictions on profiling techniques only to the use of sensitive data, and only for advertising purposes.

Second, platforms and advertisers may be tempted to bypass legal restrictions on the use of sensitive data by relying on so-called ‘proxy’ variables, i.e. seemingly neutral data points that can nonetheless serve as indicators of sensitive attributes.

⁵⁹³ Edwards and Veale (n 591) 33. See also *infra*: Section 2.2.

⁵⁹⁴ DSA, Recital 69.

⁵⁹⁵ Geese (n 555) 71.

⁵⁹⁶ Geese (n 555) 70.

For example, a person's location history, online activity, or purchasing habits may indirectly reveal sensitive characteristics such as their political views, religious beliefs, or health conditions. This is connected to the ambiguity surrounding situations in which sensitive attributes emerge as the output of an automated profiling process. In other words, what happens when profiling infers sensitive information from data that are not, in themselves, sensitive?⁵⁹⁷ However, the preamble of the DSA, Recital 69, seem to include this type of profiling within the scope of the prohibition, when stating that: '[...] providers of online platforms should not present advertisements based on profiling [...], using special categories of personal data [...], *including by using profiling categories based on those special categories*'.

Finally, in the age of 'big data', distinguishing sensitive data within vast datasets can prove challenging. Internal Facebook documents leaked through Frances Haugen's whistleblowing activity revealed that the company struggled to identify the different types of data it was storing and using. According to one of the leaked documents, a Facebook engineer stated:

*We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.' And yet, this is exactly what regulators expect us to do.*⁵⁹⁸

This means that the implementation of these provisions could require significant adaptation in platforms' internal systems. In any case, the Court of Justice of the European Union ruled that when data is processed collectively *en bloc* and it is not possible to distinguish among different categories, all such data should be treated

⁵⁹⁷ Edwards and Veale (n 591) 37.

⁵⁹⁸ Lorenzo Franceschi-Bicchieri, 'Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document' *VICE* (26 April 2022) <<https://www.vice.com/en/article/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes/>> accessed 3 February 2025.

under Article 9 of the GDPR.⁵⁹⁹ If applied more broadly, this principle implies that, whenever such a distinction cannot be made, a higher standard of protection should apply, including in the context of DSA's implementation.

As for Article 28 of the DSA, it begins with a general obligation for online platform providers to adopt appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors using their services. The second part of the article prohibits platforms from targeting online advertisement based on profiling when they are aware with reasonable certainty that the recipient of the service is a minor. At the same time, it explicitly states that platforms are not required to collect additional personal data to determine whether a user is a minor. Unlike Article 26, in this case, profiling for advertisement purposes is entirely prohibited, regardless of the type of data used. However, since only profiling is restricted, it appears that contextual targeting remains possible. This raises a broader issue, as the provisions analysed concern only profiling-based advertising, potentially leaving contextual advertising based on sensitive data, including the user's status as a minor, outside the scope of the DSA's prohibitions.

Right to an option of recommender systems not based on profiling

For VLOPs and VLOSEs, Article 38 of the DSA requires that, where recommender systems are employed, users must be offered at least one option for using the services without reliance on profiling. Despite the conciseness of this provision, it represents one of the most significant rules concerning recommender systems, as granting users to access to an unfiltered version of information reduces platforms' gatekeeping power, decreases the risk of manipulation, and enhances awareness of how algorithms shape information transmission. At the same time, this requirement strikes at the core of platforms' business model, as described in the introduction of this chapter, because it undermines their ability to monetise user engagement. For

⁵⁹⁹ CJEU, *Meta platforms and Others* (n 632), §89.

this reason, this provision has been strongly criticised by Big Tech, which argued that non-personalized recommendations would reduce customers' satisfaction and weaken their competitiveness.⁶⁰⁰ In particular, Amazon, in the proceeding initiated to annul its designation as VLOP,⁶⁰¹ argued that this provision would '*alter one of the fundamental pieces of software underpinning its business*', thereby causing a significant competitive disadvantage compared with online marketplaces that are not designated as VLOP.⁶⁰² According to Amazon's reasoning, customers may opt-out from profiling practices without being fully aware of the consequences of such a decision, subsequently assuming that their negative shopping experience reflects deficiency on the part of the provider, and ultimately turning to competitors, thereby causing a reduction of Amazon's market share.

This argument, however, appears ill-posed. Depending on how many users exercise this opt-out option, major platforms could experience a substantial decrease in their capacity to target advertisements effectively, leading to a corresponding reduction in advertising revenue. A decline in market share within the advertising sector is indeed possible, as advertisers may shift to smaller providers capable of targeting a narrower audience but more efficiently. Conversely, a comparable reduction in the user base appears less likely, as users who choose to opt out of profiling practices indicate they place limited value on personalisation and are thus unlikely to abandon the platform solely on that basis.

When examining the current implementation of this rule, its impact does not appear however to be particularly disruptive.⁶⁰³ Using again Instagram as an example, since March 2022 users have been able to switch their feed display from the default

⁶⁰⁰ Aleksandra Guzik and Linda Weigl, 'In Brussels We Trust? Preliminary Insights Into the Legal Challenges to the DMA and DSA' (*Tech Policy Press*, 5 November 2024) <<https://techpolicy.press/in-brussels-we-trust-preliminary-insights-into-the-legal-challenges-to-the-dma-and-dsa>> accessed 3 February 2025.

⁶⁰¹ See also *supra*: Section 1.1.

⁶⁰² *Amazon Services Europe Sàrl v European Commission* (n 587) §29-40.

⁶⁰³ Reviglio and Fabbri (n 571).

‘For you’ option to the ‘Following’ option in order to comply with this requirement.⁶⁰⁴ When selecting the latter, the content displayed consists solely of material from accounts the user follows, shown in chronological order. The same option is also available on TikTok.⁶⁰⁵ Although this feature may enhance the understanding of the content users see, or do not see, due to algorithmic filtering, it remains unclear how many users actually make use of this option or are even aware of its existence.

To conclude the discussion on the DSA’s restrictions on platforms’ profiling activities, it is evident that these provisions represent a shift away from the data protection framework established by the GDPR, which primarily revolves around user consent. Unlike the GDPR, the DSA does not mention consent, considering it an insufficient safeguard both from an individual perspective, since the dominance of major platforms has shown that obtaining user consent is relatively easy,⁶⁰⁶ and in terms of broader societal protection.

After outlining the restrictions on profiling imposed by the DSA, the next paragraph is dedicated to the rules on systemic risk assessment. The provisions analysed so far illustrate how the EU has identified and addressed what it considers the most significant risks through a top-down approach. However, the DSA also requires major platforms to take an active role in identifying and mitigating additional risks that may emerge from the services they provide.

1.3. SYSTEMIC RISKS ASSESSMENT ON RECOMMENDER SYSTEMS

The provisions on systemic risks outlined in Article 34 and 35 of DSA have been extensively discussed in Chapter I, Section 2.4, and Chapter 0, Section 2, with a primary focus on illegal content and content moderation activities. While there

⁶⁰⁴ Information can be found here: Adam Mosseri, ‘Control Your Instagram Feed with Favorites and Following’ (*Instagram Blog*) <<https://about.instagram.com/blog/announcements/favorites-and-following>> accessed 7 February 2025.

⁶⁰⁵ Reviglio and Fabbri (n 571).

⁶⁰⁶ More on this topic *infra*: Section 2.2.

remains debate over whether these provisions impose a duty on platforms to combat illegal content through content removal,⁶⁰⁷ it is clear that they explicitly require platforms to assess and mitigate systemic risks arising from their recommender systems, including their influence on the spread of illegal content and their potential impact on human rights, human dignity, democracy, civic debate, and electoral processes. In addition to algorithms and recommender systems, platforms must also assess risks related to advertising and data practices, which are closely interconnected.

In this framework, platforms should evaluate risks stemming from both the design of their algorithmic systems and their potential abuse by malicious actors. Regarding design, platforms are required to assess whether certain features inherently generate harmful consequences. This could be the case for algorithms primarily designed to maximise engagement, which may, for this reason, promote extreme content or create '*rabbit hole*' effects, as discussed in the opening of this chapter. Regarding abuse by malicious actors, platforms must assess whether their algorithmic systems contain vulnerabilities that could be exploited by third parties to generate undesirable effects on individuals or society.

The requirement to assess design-related risks is crucial, as it directly challenges platforms' business models, compelling them to evaluate its potential negative impacts.⁶⁰⁸ This is also linked to the issue of design-liability, meaning that while platforms cannot be held liable for third-party content, they can still be held accountable for their conduct, i.e. the way they choose to design their products. However, examining the first risk assessment reports publicly available,⁶⁰⁹ some

⁶⁰⁷ Chapter II, Section 2.4.

⁶⁰⁸ Geese (n 555) 69.

⁶⁰⁹ For some considerations on the first risk assessment reports, see: John Albert, 'DSA Risk Assessment Reports: A Guide to the First Rollout and What's next' (*DSA Observatory*, 9 December 2024) <<https://dsa-observatory.eu/2024/12/09/dsa-risk-assessment-reports-are-in-a-guide-to-the-first-rollout-and-whats-next/>> accessed 7 February 2025. It must be noted that the publicly available

scholars noted that they primarily focused on harmful behaviour and abuse, largely omitting how platform design itself intersects with main risks.⁶¹⁰

The European Commission has issued several requests for information under the DSA specifically concerning recommender systems,⁶¹¹ highlighting the sensitivity and complexity of this issue. For instance, it requested YouTube and Snapchat to provide detailed information on the role of their algorithms in amplifying risks related to, *inter alia*, civic discourse and users' mental well-being, including addictive behaviour and content 'rabbit holes'. Addictive design is one of the most crucial issues related to recommender systems,⁶¹² and was the object of an opening of proceeding against TikTok and particularly its 'Task and Reward Program'.⁶¹³ Additional concerns that could be addressed in the context of systemic risks management obligations are bias in the algorithms used for content moderation and ranking, as well as the discoverability of public interest content.⁶¹⁴ In any case, these issues are still evolving: the Commission's actions have initiated a broader dialogue, from which new mitigation measures may eventually emerge.

version may differ from the one transmitted to the European Commission, as the publication is made on a voluntary basis.

⁶¹⁰ Peter Chapman, 'Advancing Platform Accountability: The Promise and Perils of DSA Risk Assessments' (*Tech Policy Press*, 9 January 2025) <<https://techpolicy.press/advancing-platform-accountability-the-promise-and-perils-of-dsa-risk-assessments>> accessed 31 January 2025. According to someone this is particularly true for Meta's platforms, and less for others such as YouTube (Tim Bernard, 'Reading the Systemic Risk Assessments for Major Speech Platforms: Notes and Observations' (*Tech Policy Press*, 20 December 2024) <<https://techpolicy.press/reading-the-systemic-risk-assessments-for-major-speech-platforms-notes-and-observations>> accessed 7 February 2025.)

⁶¹¹ European Commission, 'Commission Sends Requests for Information to YouTube, Snapchat, and TikTok on Recommender Systems under the Digital Services Act' <<https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-youtube-snapchat-and-tiktok-recommender-systems-under-digital>> accessed 7 February 2025.

⁶¹² Chapman (n 610).

⁶¹³ European Commission, 'Commission Opens Proceedings against TikTok under the DSA' (*European Commission*, 22 April 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2227> accessed 13 October 2025.

⁶¹⁴ Damian Tambini and Eleonora Maria Mazzoli, 'Prioritisation Undercovered. The Discoverability of Public Interest Content Online' (Committee of Experts on Media Environment and Reform, Council of Europe 2020) DGI(2020)19 <<https://www.coe.int/en/web/freedom-expression/-/discoverability-of-public-interest-content-online>> accessed 13 November 2024.

Recommender systems and profiling practices are not only regulated by the DSA, but they are also addressed by the DMA. Therefore, while pursuing a different purpose, namely the competitiveness of digital markets, certain DMA provisions also impact on large digital platforms' content curation practices.

2. THE DMA RESTRICTIONS ON THE USE OF DATA AND THEIR IMPACT ON RECOMMENDER SYSTEMS

The Digital Markets Act has introduced a set of rules restricting the use of user data by platforms services that fall under the qualification of *gatekeepers*. The main objective of this Regulation is to ensure fair and contestable markets, primarily by limiting abusive practices by major online platforms. This goal is shared with traditional antitrust law, which, however, has faced certain shortcomings in the current digital ecosystem that have hindered its effectiveness.⁶¹⁵ In this context, the main contributions of the DMA compared to conventional antitrust law lies in the *ex ante* designation of dominant actors under the label of *gatekeepers*,⁶¹⁶ accompanied by a detailed list of prohibitions and obligations. The inclusion of data-related provisions in this list is unsurprising when considering that data constitute a critical asset for competition in digital markets.⁶¹⁷ Indeed, cases of data misuse have already been subject to antitrust litigation, as exemplified by the *Meta platforms* case.⁶¹⁸

Setting the DMA within the broader framework of this thesis, it can be observed that the Regulation's overarching objective of limiting platform dominance also contributes to the broader goal of constraining the opinion power of digital intermediaries. By curbing the concentration of economic power in the hands of a few dominant actors, the DMA indirectly mitigates their capacity to influence the circulation of information and shape public discourse. From this perspective, the

⁶¹⁵ See: Manzini (n 29) 324.

⁶¹⁶ See *infra*: Section 2.1.

⁶¹⁷ Manzini (n 29) 321.

⁶¹⁸ See *infra*: Section 2.2.

DMA and the DSA appear as complementary instruments. This section focuses specifically on the DMA's restrictions concerning the collection and use of data, as these rules directly affect the functioning of recommender systems and, consequently, the ways in which information is prioritised and transmitted online.

Before delving into the restrictions on the use of data introduced by the DMA (Section 2.2), it is relevant to analyse its scope, which is determined through the classification of 'gatekeeper' (Section 2.1). This concept is primarily designed to target what is commonly known as 'Big Tech' or 'GAFAM', whose dominant position is often difficult to establish under antitrust law. Notably, the gatekeeper designation serves a similar purpose to that of VLOPs and VLOSEs under the DSA, as both classifications rely on platform size for imposing additional obligations. However, the two concepts do not coincide, as explained in the following paragraph.

2.1. GATEKEEPERS VS. VLOPs AND VLOSES

Despite their conceptual similarities, a comparison between the criteria for designating gatekeepers and VLOPs/VLOSEs reveals several differences. In both cases, designation is made by the European Commission, but while the VLOPs and VLOSEs' classification relies solely on a threshold of 45 million average monthly active users,⁶¹⁹ the DMA requires additional criteria for presuming a gatekeeper position.⁶²⁰ First, it establishes also a threshold of yearly active *business* users on the platform service, which must be at least 10,000. Second, both user thresholds must have been met for three consecutive financial years, thereby demonstrating an entrenched and durable market position. Third, the platform service must operate in at least three Member States – a requirement that poses however little challenge for large online platforms that typically operate transnationally. Finally, the undertaking providing the platform service must have achieved an annual EU

⁶¹⁹ DSA, Article 33.

⁶²⁰ DMA, Article 3.

turnover of at least 7,5 billion euros over the last three years, or a market capitalisation of at least 75 billion euros in the previous financial year.

Notably, it is the undertaking providing the platform service that is designated as a gatekeeper and becomes subject to the DMA's obligations, even though the designation applies specifically to one or more of its platform services. The platform services eligible for the gatekeeper designation are listed in Article 2 and referred to as '*core platform services*'. This list includes search engine, social networks, interpersonal communications services, operating systems, video-sharing platforms, browsers, virtual assistants, clouds, online advertising services, and online intermediation services. Consequently, the classification of core platforms services under the DMA and online platforms under the DSA do not fully overlap. As of now, seven undertakings have been designated as gatekeepers, covering 24 platform services.⁶²¹

With these characteristics in mind, and despite the differences outlined, it is evident that many gatekeepers also qualify as VLOPs and VLOSEs (Appendix; Figure 8). This includes social networks (LinkedIn, Facebook, Instagram, TikTok), various intermediators (Amazon Marketplace, Google Shopping, Google Play, App Store, Google Maps, Booking.com, apart from Meta Marketplace), video-sharing platforms (YouTube), and search engines (Google Search). However, some platform services qualify as gatekeepers under the DMA but are not considered online platforms under the DSA. These include operating systems (Google Android, iOS, iPad iOS, Windows PC OS), personal communications services (WhatsApp, Messenger), browsers (Google Chrome, Safari), and advertisers (Google, Amazon, Meta).

⁶²¹ All information on gatekeeper designation can be found in the European Commission official website: European Commission, 'DMA Designated Gatekeepers' (*European Commission*) <https://digital-markets-act.ec.europa.eu/gatekeepers_en> accessed 13 October 2025.

As previously mentioned, the designation as a gatekeeper comes with a series of prohibitions and obligations. Among these, there are some restrictions on the use of data, which will be analysed in the following section.

2.2. RESTRICTIONS ON THE UTILISATION OF USER DATA

Under Article 5(2) of the DMA, gatekeepers must seek user consent for combining their personal data from different sources and, if such consent is refused, users should have access to an equivalent alternative. These provisions follow the purpose to limit gatekeeper privileged position on the market connected to its capacity to accumulate and monetise personal data coming from a wide set of services, thereby raising barriers to entry in the market.⁶²² However, the same provisions impact on the functioning of recommender systems, which traditionally were built on the combination of data from all possible sources. This groundbreaking rule has sparked considerable debate, particularly in relation to implementation on Meta's platforms through the '*pay or consent*' model.

The prohibition of combining personal data without user consent

Article 5(2) of the DMA restricts several combinations of users' data, unless users are presented with a specific choice in this regard and subsequently give their consent in accordance with the GDPR.⁶²³ The first limitation concerns the use of data for advertisement purposes and applies to data collected from third parties' services which are available on the gatekeeper's platform.⁶²⁴ This is coupled with a general restriction for combining data coming from third parties' services⁶²⁵ and from different services of the same company (e.g., Facebook and Instagram).⁶²⁶ It

⁶²² DMA, Recital 36.

⁶²³ GDPR, Article 4(11) and Article 7.

⁶²⁴ DMA, Article 5(2), a).

⁶²⁵ DMA, Article 5(2), c).

⁶²⁶ DMA, Article 5(2), b) and c).

is also specified that the gatekeeper must avoid signing-in users to other platforms services to combine personal data.⁶²⁷

These combinations of personal data are not entirely prohibited, because the gatekeeper can lawfully perform them if it obtains users' specific consent or demonstrate another legitimate basis under the GDPR. Regarding alternative legitimate basis beyond consent, the DMA explicitly references only certain grounds established by Article 6(1) of the GDPR – specifically, letters (c), (d), and (e) – omitting (b) and (f). This means that a lawful basis for such data processing can only be related to compliance with a legal obligation, protection of a persons' vital interest, or performance of tasks carried out in the public interest. The execution of contractual obligations and the legitimate interest of the processor, conversely, do not qualify as valid grounds for the data processing-practices mentioned in Article 5(2) of the DMA.⁶²⁸

When it comes to user consent, the DMA primarily refers to Article 4(11) of the GDPR, which defines consent as a freely given, specific, informed and unambiguous indication of will, as well as Article 7, which sets out the conditions for a valid consent. Additional details on the nature of user consent can be found in the DMA's preamble, which states that gatekeepers must allow users to freely opt-in to such data processing and sign-in practices by offering a *less personalised but equivalent alternative*,⁶²⁹ meaning that the use of the core platform service or its functionalities must not be conditional on user consent. More precisely, the less personalised but equivalent alternative must *not be different or of degraded quality* compared to the service provided to the users who gave consent, except where the degradation of quality is a *direct consequence* of the gatekeeper's inability to process such personal data.⁶³⁰ From this, it follows that the essence of consent under

⁶²⁷ Article 5(2), d).

⁶²⁸ This is confirmed by the DMA preamble (Recital 36).

⁶²⁹ DMA, Recital 36.

⁶³⁰ DMA, Recital 37.

the DMA lies in the ability to use platform services without being forced to agree to these data processing practices.

Unlike the DSA's provisions examined in the previous paragraph, which do not rely on user consent, this DMA's rule revolves around it but strengthens its definition by emphasizing freedom of choice. The GDPR already required consent to be freely given, but, in practice, users often encountered little real choice – essentially, they could either accept data processing or give up the service altogether.⁶³¹ The DMA, in turn, clarifies the notion of consent by ensuring that users can access platform services without being forced into consenting to data processing, thereby reinforcing the genuine autonomy of user consent.

These considerations around consent and the combination of user data largely echo a case before the German national competition authority regarding Meta platforms, which was later addressed by the Court of Justice of the European Union.⁶³² This case originated from a proceeding by the *Bundeskartellamt* (the German Competition Authority) concerning Meta's practice of combining data collected on Facebook with *off-Facebook* data; specifically, data from its other services, such as Instagram, WhatsApp, and Oculus, as well as from third-party websites. The *Bundeskartellamt* found that this practice violated both the GDPR and competition law, particularly as it represented an abuse of dominant position. A German regional court then referred the case to the CJEU through a preliminary ruling request. Even though the request also included several questions on the intersection between privacy and antitrust law,⁶³³ this section specifically focuses on the concept of freely given consent under the GDPR.

⁶³¹ See *supra*: Chapter III.

⁶³² *Meta platforms and Others* [2023] Court of Justice of the European Union ECLI:EU:C:2022:704, C-252/21.

⁶³³ For a detailed analysis of all the questions addressed by the CJEU in this case, see: Pietro Manzini, 'Antitrust e Privacy: La Strana Coppia' in Pietro Manzini (ed), *I confini dell'antitrust. Diseguaglianze sociali, diritti individuali, concorrenza* (Giappichelli 2023).

According to the Bundeskartellamt, Meta's data processing practices lacked valid consent because users had no actual choice: consent was a precondition for accessing Facebook's services, and Facebook's dominant market position left users with no real alternatives.⁶³⁴ The CJEU was asked to determine whether consent could be regarded as freely given when the data controller holds a dominant position. The Court ruled that dominance *per se* does not automatically invalidate consent under the GDPR. However, for the consent to be valid, users must be free to refuse data processing practices that are not necessary for the performance of the contract and must still be allowed to access an equivalent service, potentially for an appropriate fee.⁶³⁵ Beyond the issue of consent, the CJEU also examined other possible legal basis for data processing under the GDPR, substantially ruling out that these practices could be justified as necessary for the execution of the contract,⁶³⁶ or because falling within a legitimate interest of the platform.⁶³⁷

The data processing practices at issue in the *Meta* case substantially overlap with those addressed by Article 5(2) of the DMA. The notions of consent and the availability of alternative equivalent options for accessing services are also shared. Moreover, the CJEU's exclusion of letters (b) and (f) of Article 6(1) GDPR as valid grounds for such data processing practices is likewise aligned with the DMA's provisions. One notable difference, however, is that the CJEU judgement contemplated the possibility of charging a fee for accessing services without data combination, whereas the DMA remains silent on this point. This divergence

⁶³⁴ Alessia D'Amico and others, 'Meta's Pay-or-Okay Model: An Analysis under EU Data Protection, Consumer and Competition Law' (2024) 2024 Technology and Regulation 254 <<https://techreg.org/article/view/19031>> accessed 7 February 2025.

⁶³⁵ CJEU, *Meta platforms* (n 632), §150.

⁶³⁶ CJEU, *Meta platforms* (n 632), §97-104.

⁶³⁷ CJEU, *Meta platforms* (n 632), §105-124. The EDPB also found that Meta could not rely on reasons related to the execution of contract and legitimate interests for behavioural advertising purposes: European Data Protection Board, 'Urgent Binding Decision 01/2023 Requested by the Norwegian SA for the Ordering of Final Measures Regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR)' <https://www.edpb.europa.eu/our-work-tools/our-documents/urgent-binding-decision-board-art-66/urgent-binding-decision-012023_en> accessed 18 February 2025.

created uncertainty as to whether Meta's subsequent *pay-or-consent* model, introduced in response to these regulatory developments, was compatible with the DMA's requirements, an issue analysed in the following paragraph.

Meta 'pay-or-consent' model and subsequent developments

Meta was among the first companies designated as gatekeeper by the European Commission, covering six core platform services: Facebook, Instagram, WhatsApp, Messenger, Meta Marketplace, and Meta Advertising.⁶³⁸ To comply with the DMA, and particularly with Article 5(2), Meta introduced a binary *pay-or-consent* model on its platforms in November 2023 (Appendix, Figure 6).⁶³⁹ Under this system, EU users of Facebook and Instagram received a notification inviting them to choose between: (i) paying a monthly subscription for an ad-free experience, or (ii) continuing to access the platforms free of charge agreeing with personalised advertising. As a result, users were offered a new possibility to access Meta's services without consenting to the data processing covered by the DMA, although only by paying a fee of approximately €250 per year.⁶⁴⁰

This system sparked renewed debates about users' freedom of choice, largely driven by civil-society organizations.⁶⁴¹ For instance, *noyb*, a privacy-focused NGO, highlighted that, although surveys indicated that only 3-10% of users wanted their personal data to be used for targeted advertising, 99% opted for the free version of Meta's services to avoid paying a fee,⁶⁴² an outcome indicating a

⁶³⁸ European Commission, 'Digital Markets Act: Commission designates six gatekeepers' <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328> accessed 18 February 2025.

⁶³⁹ Also referred to as 'pay-or-okay' model.

⁶⁴⁰ Noyb, 'Statement on EDPB "Pay or Okay" Opinion' (*noyb*, 17 April 2024) <<https://noyb.eu/en/statement-edpb-pay-or-okay-opinion>> accessed 18 February 2025. This fee was the lowered one year after (see footnote no. 647).

⁶⁴¹ Noyb, '28 NGOs Urge EU DPAs to Reject "Pay or Okay" on Meta' (*noyb*, 16 February 2024) <<https://noyb.eu/en/28-ngos-urge-eu-dpas-reject-pay-or-okay-meta>> accessed 18 February 2025. Similar considerations can be found here: Corporate Europe Observatory, 'How Corporate Lobbying Undermined the EU's Push to Ban Surveillance Ads' (*Corporate Europe Observatory*, 18 January 2022) <<https://corporateeurope.org/en/2022/01/how-corporate-lobbying-undermined-eus-push-ban-surveillance-ads>> accessed 21 February 2025.

⁶⁴² Noyb, 'Statement on EDPB "Pay or Okay" Opinion' (n 640).

significant constraint on the genuine voluntariness of consent. The *pay-or-consent* model also came under the scrutiny of the European Commission, which opened proceedings against Meta on 25 March 2024.⁶⁴³ In its preliminary findings, presented on 1 July 2024, the Commission considered the model non-compliant with the DMA, precisely because it failed to provide users with access to an equivalent service that uses less of their personal data and did not allow them to freely exercise their consent to data combination practices.⁶⁴⁴ The *pay-or-consent* model has also been the subject of an opinion of the European Data Protection Board, which outlined the conditions under which such system could be deemed compatible with the GDPR.⁶⁴⁵ The Commission's proceedings concluded on 23 of April 2025 with the final decision confirming the preliminary findings and imposing a €200 million fine on Meta for the period during which *pay-or-consent* was the sole option available.⁶⁴⁶ Meanwhile, the Commission is still assessing the legality of Meta's newly introduced 'ad-breaks' option, which is further discussed below.

The opening of proceedings by the Commission and the publication of its preliminary findings prompted Meta to revise its policies. In November 2024, the company not only reduced the fee required to access the ad-free version (now amounting to approximately €95 per year) but also introduced an additional option allowing users to continue using the free version with a reduced collection of

⁶⁴³ European Commission, 'Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act' <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689> accessed 18 February 2025.

⁶⁴⁴ European Commission, 'Commission sends preliminary findings to Meta over its "Pay or Consent" model for breach of the Digital Markets Act' <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3582> accessed 7 February 2025.

⁶⁴⁵ European Data Protection Board, 'Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms' <https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en> accessed 18 February 2025.

⁶⁴⁶ European Commission, 'Commission finds Apple and Meta in breach of the Digital Markets Act' (*European Commission*, 23 April 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085> accessed 29 April 2025.

personal data for advertising purposes.⁶⁴⁷ The free version now enables users to choose between a social media experience with advertisements that are either ‘more’ or ‘less’ personalized (Appendix, Figure 7). However, Meta has designed a less seamless browsing experience for users who refuse profiling-based ads. These users encounter now unskippable ‘ad breaks’ lasting several seconds while using Meta’s platforms, which significantly slows down navigation (Appendix, Figure 7).

Choosing the less-personalised version with ad breaks implies that advertisements are displayed solely on the basis of contextual data, namely what a user views during a particular session on Facebook and Instagram, together with a minimal set of data points such as age, location, gender, and ad engagement.⁶⁴⁸ This new option significantly alters the traditional functioning of recommender systems and, consequently, the way content is displayed.

The transparency obligations on advertising imposed by the DSA make it possible to compare the targeting criteria applied to users who select the more personalised option with those who opt for the less personalised one.⁶⁴⁹ A simple experiment analysing the advertisements shown to users under different settings indicates that users opting for the less personalised version (with ad breaks) receive ads based only on basic criteria such as location, age, and gender (Appendix, Figure 4). In contrast, users opting for the personalised version are targeted through profiling, which relies on data about previous activity across different platforms, as well as interactions with other ads and users (Appendix, Figure 5). However, as previously observed, despite this additional information, understanding how profiling-based

⁶⁴⁷ Meta, ‘Facebook and Instagram to Offer Subscription for No Ads in Europe’ (*Meta*, 12 November 2024) <<https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>> accessed 13 February 2025.

⁶⁴⁸ Brian O’Donovan, “Unskippable” Ads to Feature on Facebook and Instagram’ *Raidió Teilifís Éireann (Rte)* (12 November 2024) <<https://www.rte.ie/news/2024/1112/1480520-facebook-ads/>> accessed 18 February 2025.

⁶⁴⁹ DSA, Article 27. See *supra*: Section 1.1.

advertising operates remains difficult due to the vagueness of the descriptions provided.⁶⁵⁰

While the *ad-break* option is more acceptable to users compared to the paying option, its slower functioning could represent a significant disadvantage for those who use online platforms intensively, such as influencers, potentially discouraging them from opting out of profiling.⁶⁵¹ Comparing the new *ad-break* option with the *pay-or-consent* model, it appears that in both cases the reduced possibility to monetise user data is accompanied by a deliberate downgrading of the user experience by the platform provider. Although the options offered by Meta's platforms mostly emphasise content *personalisation* – framed as a service provided in the users' interest – data collection primarily benefits the platform, representing its main source of revenue.⁶⁵² Rules restricting the use of user data are groundbreaking for these platforms, as they strike at the core of their business model. Personalised advertising, based on the aggregation of cross-service and third-party data to build detailed user profiles, has been the foundation of the multibillion-dollar profits of Meta and Google. From this perspective, additional advertisements and subscription fees are presented as a form of compensation for the loss of revenue resulting from the reduced ability to monetise user data.

These developments have once again highlighted the misleading nature of Facebook's former slogan, '*It's free and always will be*', which appeared on its login page until 2019.⁶⁵³ Following regulatory scrutiny, Meta was then required to

⁶⁵⁰ See *supra*: Section 1.1.

⁶⁵¹ At the same time, they could reduce user engagement, and becoming detrimental also for the platform itself /maybe this is the reason why, based on the author's personal experience) ad-breaks are increasingly rare on the platform (26 October 2025).

⁶⁵² Zuboff (n 32) 113.

⁶⁵³ Qayyah Moynihan Asenjo Alba, 'Facebook Quietly Ditched the "It's Free and Always Will Be" Slogan from Its Homepage', *Business Insider*, 27 August 2019, <https://www.businessinsider.com/facebook-changes-free-and-always-will-be-slogan-on-homepage-2019-8>. Martina Pennisi, 'Facebook, perché sulla homepage non c'è più scritto «è gratis»', *Corriere della Sera* (28 August 2019) <https://www.corriere.it/tecnologia/19_agosto_28/facebook-perche-homepage-non-c-piu-scritto-gratis-sara-sempre-9498de42-c97a-11e9-89f2-

remove this slogan and to clarify in its terms of service that: ‘*we don’t charge you money to use our products because businesses and organizations pay us to show you ads*’.⁶⁵⁴ The introduction of subscription fees after the imposition of restrictions on data-driven monetisation confirms that personal data have long constituted the true currency for accessing these services.

Given that the new options introduced by Meta create a *de facto* disincentive for users to opt out of certain data-processing practices, their compliance with the principle of freely given consent, as outlined in GDPR and DMA, remains questionable. At the same time, one may argue that declaring these alternative monetisation models unlawful would, in practice, oblige platforms to offer their services free of charge, as if they were fulfilling a sort of public service function. However, EU regulations do not require the provision of a completely ad-free version of these services and, while they restrict profiling-based advertising, they do not limit targeting based on contextual or first-party data. Platforms could, therefore, arguably remain economically viable within this regulatory framework, even if these alternative monetisation models were to be declared unlawful.

While the DSA and DMA rules analysed in this chapter apply to all types of advertising and recommender systems, even though some of them apply only certain categories of platforms, additional, more specific rules have been introduced

27d7028d49f0.shtml> accessed 18 February 2025; Qayyah Moynihan Asenjo Alba, ‘Facebook Quietly Ditched the “It’s Free and Always Will Be” Slogan from Its Homepage’ *Business Insider* (27 August 2019) <<https://www.businessinsider.com/facebook-changes-free-and-always-will-be-slogan-on-homepage-2019-8>> accessed 18 February 2025. Martina Pennisi, ‘Facebook, perché sulla homepage non c’è più scritto «è gratis»’ *Corriere della Sera* (28 August 2019) <https://www.corriere.it/tecnologia/19_agosto_28/facebook-perche-homepage-non-c-piu-scritto-gratis-sara-sempre-9498de42-c97a-11e9-89f2-27d7028d49f0.shtml> accessed 18 February 2025; Qayyah Moynihan and Alba Asenjo, ‘Facebook Quietly Ditched the “It’s Free and Always Will Be” Slogan from Its Homepage’ *Business Insider* (27 August 2019) <<https://www.businessinsider.com/facebook-changes-free-and-always-will-be-slogan-on-homepage-2019-8>> accessed 18 February 2025.

⁶⁵⁴ Anna Benckert, ‘We’re Updating Our Terms of Service to Better Explain How Facebook Works’ (*Meta*, 27 June 2019) <<https://about.fb.com/news/2019/06/updating-our-terms/>> accessed 19 February 2025.

for political advertising through the Regulation on the transparency and targeting of political advertising. These will be examined in the following section.

3. THE REGULATION ON POLITICAL ADVERTISING

Political advertising on online platforms stands as the clearest demonstration of digital platforms' opinion power. Political advertising has always represented a democratic concern and has traditionally been regulated to ensure fair and transparent political processes.⁶⁵⁵ On platforms, political advertising is mainly disseminated through recommender systems. The rise of targeted political advertising has raised new concerns, as massive data collection enables micro-targeting based on personal preferences and vulnerabilities, thereby amplifying the potential for manipulation, as exemplified by the Cambridge Analytica scandal.⁶⁵⁶

While national regulations on political advertising have traditionally applied to offline media in this context, the need to address the online environment from a transnational perspective has emerged, particularly given the increased global demand for political advertising.⁶⁵⁷ In this context, the European Union adopted the Regulation on the Transparency and Targeting of Political Advertisement (PAR) on 13 March 2024. Its main provisions are set to enter into force in autumn 2025.⁶⁵⁸

The goal of this Regulation is to enhance the transparency of political advertising, enabling citizens to make informed decisions, preventing manipulation, and ensuring an open and free electoral process.⁶⁵⁹ Additionally, the Regulation introduces specific rules addressing online targeting techniques, which are considered a particular threat to fairness, transparency and fundamental rights, including freedom of expression, privacy and right to receive proper information.⁶⁶⁰

⁶⁵⁵ See *supra*: Chapter I, Section 2.2.

⁶⁵⁶ Described *supra*: Chapter I, Section 2.1.

⁶⁵⁷ PAR, Recitals 1, 2, 7.

⁶⁵⁸ PAR, Article 30(2).

⁶⁵⁹ PAR, Recital 4.

⁶⁶⁰ PAR, Recital 6.

In this regard, the preamble highlights the growing frequency of tailored political content that leverages both observed and inferred personal data revealing political opinions and is disseminated through often opaque algorithms.⁶⁶¹ Conversely, while offline political advertising has often been regulated also from the perspective of equality of access, this aspect is not addressed by this Regulation.⁶⁶²

To understand the impact of this Regulation, it is essential to first define its scope, beginning with the definition of political advertising itself (Section 3.1). The Regulation then outlines a series of general provisions applicable to all providers or publishers of political advertising, followed by specific provisions addressing online targeted political advertising. Given that this chapter focuses on recommender systems on major online platforms, restrictions on online targeted political advertising will first be presented (Section 3.2), before examining the broader transparency obligations imposed for the various forms of political advertising (Section 3.3).

Among the general provisions now applicable to political advertising within the EU, it is worth mentioning the one preventing external interference in electoral processes. Indeed, Article 5(2) mandates that, during the three months preceding any voting process in the EU, providers of political advertisement services must only offer services to an EU citizen, a permanent resident of a Member State, or a legal entity which is not owned or controlled by a third-country person. Since this rule also applies to online platforms, they are effectively prohibited from accepting political advertisements from outside the EU during electoral periods.

3.1. THE PROBLEM OF DEFINING POLITICAL SPEECH

Defining political advertising is challenging, as the boundaries of political discourse can be very broad, encompassing many aspects of personal and social life. Political

⁶⁶¹ PAR, Recital 6.

⁶⁶² Malgorzata Kozak, 'Regulating Political Advertising' [2023] Verfassungsblog <<https://verfassungsblog.de/regulating-political-advertising/>> accessed 10 February 2025.

opinions are shaped by a wide range of factors, and debates on these issues can significantly influence electoral processes. For regulatory purposes, however, political speech must be defined narrowly to ensure legal certainty. In this regard, the PAR appears to adopt a restrictive approach, focusing primarily on institutional political speech, namely sponsored communication by political actors *strictu sensu*, such as political parties and candidates. Yet, as discussed further below, certain elements of the definition remain unclear, giving rise to considerable debate.

The definition of political advertising provided by Article 3(2) of the PAR includes the ‘*preparation, placement, promotion, publication, delivery or dissemination*’, by any means, of a political message. It specifies that such activities are typically provided behind remuneration, through in-house activities, or as part of a political advertising campaign. Moreover, for a message to qualify as political advertisement, it must either (i) be provided by, for or on behalf of a political actor; or (ii) be suitable and designed to influence the outcome of a democratic process, including an election or referendum, voting behaviour or a legislative or regulatory process, at Union, national, regional or local level. The same article also specifies the definition of ‘political actor’, which essentially refers to institutional political actors, such as parties, candidates, and members of public institutions.⁶⁶³ Regarding geographical scope, the PAR applies when the political message is disseminated in the European Union, independently from the establishment of the provider or sponsor.⁶⁶⁴

The Regulation explicitly outlines several exclusions from the definition of political advertising. First, political opinion expressed under editorial responsibility, unless they are provided behind remuneration, together with those expressed in an individual capacity, are excluded.⁶⁶⁵ Secondly, messages from official sources of

⁶⁶³ PAR, Article 3(4).

⁶⁶⁴ PAR, Article 2(1).

⁶⁶⁵ PAR, Article 1(2) and 1(3).

Member States or the EU strictly regarding the organisation and modalities for participating in elections or referendums; public communications intended to provide official information (e.g., press releases); and messages presenting candidates in designated public spaces or in the media provided by law and free of charge, while ensuring the equal treatment of candidates, are also not considered political advertisement.⁶⁶⁶

Moreover, there is a general exclusion for messages of a purely private or purely commercial nature. To assess the nature of the message, all relevant factors must be taken into consideration, including its content, the sponsor, the language used, the context (including the period of dissemination), the objective of the message, the means of transmission, and the targeted audience.⁶⁶⁷ The European Commission may also develop guidelines to ensure the correct interpretation of these criteria.

The distinction between private and political opinions is likely to be one of the most contentious issues.⁶⁶⁸ However, the changes made to the original proposal can provide guidance for interpretation. The preamble of the proposal initially stated that messages on societal or controversial issues which could influence electoral processes should be considered political advertising,⁶⁶⁹ leading to the substantial inclusion of non-remunerated content.⁶⁷⁰ In contrast, civil society organisations argued that only paid or sponsored political content should be regulated, expressing concerns that including all public interest content, including messages related to abortion, animal protection or human rights, could refrain civil society

⁶⁶⁶ PAR, Article 3(2). See also: Recitals 27 and 28.

⁶⁶⁷ PAR, Article 8 and Recital 22.

⁶⁶⁸ Vincenzo Iaia, 'I Complessi Contorni Della Nozione Di Pubblicità Politica Alla Prova Delle Elezioni Europee 2024' (*MediaLaws*, 19 June 2024) <<https://www.medialaws.eu/21061-2/>> accessed 24 February 2025.

⁶⁶⁹ Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising, COM/2021/731 final, Recital 17.

⁶⁷⁰ Sebastian Becker, 'Political Negotiations Continue: EU Lawmakers Fail to Agree on Strong Rules for Regulating Political Advertising' (*European Digital Rights (EDRi)*, 12 October 2023) <<https://edri.org/our-work/political-negotiations-continue-eu-lawmakers-fail-to-agree-on-strong-rules-for-regulating-political-advertising/>> accessed 21 February 2025.

organisations from generating and disseminating unpaid political messages, ultimately discouraging free speech and activism.⁶⁷¹ Following these debates, lawmakers agreed to keep non-commercial political speech mostly out of scope of the PAR, establishing that political advertisement is *normally* provided behind remuneration. However, non-remunerated content has not been entirely excluded, particularly regarding so-called *in-house* activities, i.e. activities carried out *within* a political entity to convey a political message.⁶⁷² This could, for example, apply to a political party promoting its own content, which, being done in its own interest, does not involve remuneration. However, the interpretation of this provision remains open and could be applied more broadly.

Having presented the PAR's scope and possible uncertainties to this regard, its main provisions regarding recommender systems are illustrated in the next paragraphs.

3.2. LAWFUL TARGETED POLITICAL ADVERTISEMENT: EXPLICIT CONSENT AND RESTRICTIONS ON PROFILING

As previously mentioned, the PAR includes specific provisions regulating online targeted political advertising. Targeting is defined as a technique that delivers content selectively, i.e. only to a specific person or group of persons, or through selective exclusions, based on the processing of personal data.⁶⁷³ The connection between targeting and personal data is made clear from this definition, which is why the main rules of the PAR are built upon the GDPR framework, with their enforcement entrusted to national data protection authorities.

The requirements for the lawful use of online targeted political advertising based on the processing of personal data are set out in Article 18 of the PAR, which establishes three key requirements. First, the controller must have collected the

⁶⁷¹ Article 19, 'The Implication of the Proposed EU Political Advertising Regulation for Freedom of Expression' <https://www.article19.org/wp-content/uploads/2023/08/A19-The-implications-of-the-Proposed-EU-Political-Advertising-Regulation-A19_clean.pdf>.

⁶⁷² PAR, Recital 24.

⁶⁷³ PAR, Article 3(11).

personal data directly from the data subject, thereby excluding data obtained from third parties. Second, the data subject must have given *explicit* and *separate* consent to this kind of data processing in accordance with the GDPR. Third, profiling based on the special categories of data listed in Article 9 of the GDPR is strictly prohibited for the purpose of targeting political advertising.⁶⁷⁴ In addition, targeted political advertisement is prohibited when the controller has reasonable certainty that the recipient is at least one year below the voting age.⁶⁷⁵ This restriction is justified by their particular vulnerability of younger individuals and the associated risk of influencing them to manipulate public debate.⁶⁷⁶

The following paragraphs illustrate the second and third requirements, namely the need for specific content and the prohibition on the use of sensitive data for targeting political advertising.

Explicit and separate consent for targeted political advertising

The consent that online providers must obtain for targeting political advertising must not only meet all the requirements set by GDPR but also be requested separately. The Regulation further specifies that the consent should be required only once, unless there is a substantial changing of circumstances, and that revoking consent must not be harder than giving it.⁶⁷⁷ Repeatedly prompting users for consent is considered a *dark pattern*, as it may nudge them into making a choice they would not have otherwise made.⁶⁷⁸ Additionally, the fact that a data subject has voluntarily disclosed their data cannot be considered a sufficient legal ground for political targeting practices.⁶⁷⁹

⁶⁷⁴ It is explicitly provided that these rules do not apply to non-profit parties and associations for the communication addressed to their members: PAR, Article 18(3).

⁶⁷⁵ PAR, Article 18(2).

⁶⁷⁶ PAR, Recital 82.

⁶⁷⁷ PAR, Article 18(4), Recital 80

⁶⁷⁸ PAR, Recital 75.

⁶⁷⁹ PAR, Recital 80. Conversely, the GDPR includes voluntary disclosure as legitimate basis for processing special categories of data under Article 9(2), lett. *e*).

Moreover, to ensure that consent is genuinely freely given, the Regulation reiterates the requirement to provide an ‘equivalent alternative’ to the service offered. Online providers are thus required to allow users to opt out from political advertising while continuing to use their services.⁶⁸⁰ In this regard, the preamble explicitly references the *Meta Platforms* case.⁶⁸¹

The prohibition of profiling based on sensitive data for targeted political advertising

Another key rule concerning targeted political advertising is the *outright* prohibition of profiling based on the special categories of data listed in Article 9 of the GDPR. A complete prohibition implies that the exceptions provided in Article 9 GDPR are not applicable in this context and therefore cannot serve as a legitimate basis for data processing.⁶⁸² Consequently, providers cannot rely on user consent to target political advertising using sensitive data,⁶⁸³ aligning this rule with Article 26 of the DSA, which already prohibits profiling on online platforms based on sensitive data for advertising purposes.⁶⁸⁴ However, the PAR extends this rule to any online provider of political advertising.

Notably, unlike the DSA, the PAR explicitly states that the prohibition applies both when special category of data are collected directly, and when they are inferred from the processing of non-special personal data.⁶⁸⁵ Furthermore, the prohibition extends to any data revealing such sensitive information, regardless of how they are labelled, and applies independently of the accuracy of the categorisation. However, as mentioned earlier regarding the DSA,⁶⁸⁶ distinguishing between different

⁶⁸⁰ PAR, Article 18(4), Recital 81.

⁶⁸¹ See *supra*: Section 2.2.

⁶⁸² PAR, Recital 77.

⁶⁸³ Becker (n 670).

⁶⁸⁴ See *supra*: Section 1.2.

⁶⁸⁵ Recital 79.

⁶⁸⁶ See footnote n 684.

categories of data may not be very effective. This is a concern shared by certain civil society organisations.⁶⁸⁷

3.3. TRANSPARENCY OBLIGATIONS ON POLITICAL ADVERTISING FOR ONLINE PLATFORMS

As previously anticipated, the PAR establishes several transparency obligations for political advertising, some of which apply to all providers, while others impose additional requirements on online platforms and on targeted political advertisement. The following paragraph outlines the main provisions concerning transparency obligations for online platforms in the context of political advertising.

First, all providers of political advertising must require advertisers to declare whether the requested advertising services qualifies as political under the PAR.⁶⁸⁸ Any contract subsequently concluded must comply with the rules established by the Regulation and, where an online interface is used, it must be designed in a way that ensures compliance.⁶⁸⁹ Providers are also required to retain records of the information related to the delivery of the requested advertising service for seven years. These records must include the content of the advertisement, the identity of the sponsor, and electoral or political process to which the advertisement relates.⁶⁹⁰

Additional obligations apply to publishers of political advertising, a category that includes services that publish, deliver, or disseminate political advertising through any medium.⁶⁹¹ These actors generally operate at the final stage of the distribution process, and include online platforms. Publishers must ensure that every political advertisement is accompanied by clear, salient and unambiguous information

⁶⁸⁷ Asha Allen, 'New EU Rules on Political Advertising Set to Have Limited Impact on Advertising Ecosystem' (*Center for Democracy and Technology*, 20 March 2024) <<https://cdt.org/insights/new-eu-rules-on-political-advertising-set-to-have-limited-impact-on-advertising-ecosystem/>> accessed 20 February 2025.

⁶⁸⁸ PAR, Article 8.

⁶⁸⁹ PAR, Article 7(2) and (5).

⁶⁹⁰ PAR, Article 9.

⁶⁹¹ PAR, Article 3(13).

identifying it as such. Moreover, such information must disclose whether the advertisement is targeted, specify the identity of the sponsor and, where possible, the entity ultimately controlling the sponsor, as well as indicate the political process (for example, an election or a referendum) to which the advertisement relates.⁶⁹²

Other information about political advertising must be included in a transparency notice, which must be linked or easily accessible from the sponsored content. This notice must contain details about the sponsor, the paying entity, the advertising period, the amount of money spent, the origin of the funds, the electoral processes at stake, and information on how to participate to such electoral process.⁶⁹³ Publishers are responsible for ensuring the completeness of all information and the accuracy of those details under their control. If they find any inaccuracies or missing information, they must request corrections from the sponsor. If the sponsor fails to comply, the advertisement must not be published.⁶⁹⁴ Online providers designated as VLOP or VLOSE in line with the DSA are required to include the transparency notice in the advertising repository mandated by Article 39 of the DSA.⁶⁹⁵ A European repository for online political advertisements is also established by the European Commission.

For data controllers using targeting techniques for online political advertising, Article 19 imposes specific additional transparency obligations. According to this provision, along with the clear indication that the content is a political advertisement, individuals must be able to access information about the logic and parameters of targeting. This includes a disclosure on the specifically targeted groups, the categories of personal data used, the targeting mechanism, the reasons for selecting certain parameters, and a link to an internal policy document explaining the targeting techniques. Data controllers are also required to conduct an

⁶⁹² PAR, Article 11.

⁶⁹³ PAR, Article 12(1).

⁶⁹⁴ PAR, Article 12(2). See *supra*: Section 1.1.

⁶⁹⁵ PAR, Article 13(2).

internal risk assessment to evaluate the impact of their targeting mechanism for political advertising on fundamental rights and freedoms.

Article 17 grants researchers, journalists, civil society organizations, electoral observers, and politicians, the right to request information from publishers, who must provide it free of charge within one month unless providing a reasoned response justifying that they do not possess the requested information or that the request is unclear. The same right is also recognized regarding data on targeted political advertisement.⁶⁹⁶

Moreover, publishers must implement mechanisms allowing individuals and organizations to report political advertisement that do not comply with the PAR, facilitating precise and substantiated notifications.⁶⁹⁷ Certain obligations are enhanced for publishers qualifying as VLOPs and VLOSEs: they must handle these notifications diligently, objectively, non-arbitrarily and without undue delay, informing the notifier of the follow-up. In the month preceding an electoral process, such notifications must be addressed within 48 hours.

In summary, the PAR imposes to online platforms an obligation to clearly label political advertising and provide users with information explaining why they are receiving content, with particular emphasis on whose behalf it is being promoted. Interestingly, the regulation assigns publishers a role in the public interest by mandating them to provide information on how to participate in electoral processes, effectively making them facilitators of democratic engagement. Oversight on transparency obligations is partially entrusted to users, who are given the ability to report non-compliance. However, the short timeframe for content removal during electoral period raises concerns. While intended to prevent the spread of unlawful

⁶⁹⁶ PAR, Article 20.

⁶⁹⁷ PAR, Article 15.

political advertising, it creates a risk of over-removal of content, which in turn poses an equal threat to the integrity of public debate.⁶⁹⁸

CONCLUDING REMARKS

Recent EU regulations on digital platforms, including the DSA, the DMA and the Regulation on Political Advertising, contain several provisions governing recommender systems. These rules can broadly be divided into two categories: those restricting the collection and the use of the data that feed algorithmic systems, and those enhancing transparency requirements.

Regarding the first category, this chapter illustrated several restrictions on data processing, resulting in a complex regulatory framework. While most of these rules differ in scope, both in terms of the type of data processing regulated and the entities subject to compliance, overlaps can be observed. The following table summarises the key provisions analysed, aiming to provide a clearer overview of the current regulatory landscape.

Table 1. Restrictions on data processing under different EU regulations affecting digital platforms

Regulation	Type of Data Processing	Compliance Requirements	Subject Entities
GDPR – Art. 6	Any data processing	Legitimate basis	All data processors
GDPR – Art. 9	Processing special categories of data	Prohibited with exceptions	All data processors
DSA – Art. 26	Profiling based on special categories of data for the purpose of ad	PROHIBITED	Online platforms
DSA – Art. 28	Profiling minors for the purpose of ad	PROHIBITED	Online platforms

⁶⁹⁸ Allen (n 687); Article 19 (n 671).

DSA – Art. 38	Profiling for recommender systems	Need to provide an alternative	VLOPs and VLOSEs
DMA – Art. 5(2)	Combining data from different sources	Need to provide an equivalent alternative	Gatekeepers
PAR – Article 18	All online targeted political advertisement	Specific and separate consent + equivalent alternative	All data processors
PAR – Article 18	Online targeted political ad based on profiling + on data collected by third parties	PROHIBITED	All data processors

This summary highlights how the founding principles established by the GDPR in 2016 for personal data processing have evolved along two key directions. First, additional safeguards have been introduced to ensure that user content is genuinely free, thereby reinforcing individual autonomy. In this respect, Article 38 of the DSA,⁶⁹⁹ Article 5(2) of the DMA,⁷⁰⁰ and Article 18 of the PAR,⁷⁰¹ all require digital service providers to offer an *equivalent alternative* that involves less extensive data collection practices. Second, certain types of personal data processing have been outright prohibited, irrespective of user consent. Notably, Article 26 of the DSA prohibits profiling based on sensitive data for advertising purposes, while Article 28 prohibits any profiling for advertising purposes when directed at minors.⁷⁰² This regulatory shift marks a decisive move away from a purely contractual model based on the formal freedom of the parties, aligning instead with legal frameworks addressing structural contractual asymmetries, such as consumer protection and competition law.

In addition to rules on data processing, there is a second category of provisions imposing transparency obligations regarding recommender systems, as those

⁶⁹⁹ See *supra*: Section 1.2

⁷⁰⁰ See *supra*: Section 2.2

⁷⁰¹ See *supra*: Section 3.2

⁷⁰² See *supra*: Section 1.2

established by Articles 26 and 27 of the DSA and Article 18 of the PAR.⁷⁰³ The protection of user privacy is thus complemented with measures aimed at empowering them through a greater understanding of algorithmic recommendations. Providing users with information about the functioning of digital platforms' filtering power enhances external scrutiny and helps identify potential bias or manipulation.

The risk of manipulation is one of the main concerns addressed by these regulations, not only from an individual perspective but also with the broader aim of mitigating societal risks, including threats to the integrity of democratic processes. This explains why individual consent is not considered a sufficient legal basis for certain types of data processing, which are regarded as particularly dangerous, particularly when carried out on a large scale. A major area of concern in this regard is represented by '*surveillance-based advertising*', which relies on extensive data collection, behavioural profiling, predictive analytics and microtargeting, with the purpose to influence user choices, often without their full awareness or meaningful control. While recent regulations have introduced significant limitations to these practices, particularly concerning targeted advertising using sensitive data, some observers argue that they remain insufficiently addressed.⁷⁰⁴

Moreover, while the exercise of gatekeeping power has become increasingly transparent, the functioning of recommender systems remains largely determined unilaterally by platforms. Users can choose to receive less personalised advertising,⁷⁰⁵ refuse targeted political advertising,⁷⁰⁶ and access an unfiltered version of major platform services,⁷⁰⁷ but these solutions represent rigid binary

⁷⁰³ See *supra* respectively: Section 1.1 and Section 3.3

⁷⁰⁴ Becker and Penfrat, 'The DSA Fails to Reign in the Most Harmful Digital Platform Businesses – But It Is Still Useful'; and 'How Corporate Lobbying Undermined the EU's Push to Ban Surveillance Ads'.

⁷⁰⁵ DMA, Article 5(1).

⁷⁰⁶ PAR, Article 18.

⁷⁰⁷ DSA, Article 38.

choices, rather than opportunities to actively personalise recommendation parameters according to individual preferences.⁷⁰⁸ Indeed, the degree of actual control conferred upon users on recommender systems remains limited, since the DSA only requires transparency about existing options to influence their parameters, but does not oblige providers to offer such options in the first place.⁷⁰⁹ In any event, this chapter has illustrated some cases where platforms do provide such options; however, in the absence of a legal obligation to do so, these remain rather limited.

It must be noted that, in the context of systemic risks assessment concerning the functioning of recommender systems and algorithms, major digital platforms (VLOPs and VLOSEs) may ultimately be required to adopt additional measures to address their impact on public opinion.⁷¹⁰ Whether such measures will be required depends both on the assessments carried out by the platforms themselves and on the subsequent scrutiny exercised by the European Commission. This observation reflects a broader point: beyond the formal regulatory framework, the practical implementation of rules by platforms and their enforcement by supervisory authorities are decisive in determining their actual impact.

It also noteworthy that, while the DSA imposes significant transparency obligations regarding the functioning of recommender systems, no comparable provisions exist under the AI Act, including with respect to generative AI systems and their content selection practices. The AI Act contains only a few transparency requirements under Article 50, which mandates that users are informed when interacting with an AI system, and that artificially generated content and *deepfakes* are appropriately disclosed. At the same time, providers of AI systems are not subject to restrictions on data combination for the purpose of targeting recommendations, as they do not

⁷⁰⁸ Reviglio and Fabbri (n 571).

⁷⁰⁹ See *supra*: Section 1.1

⁷¹⁰ See *supra*: Section 1.3

per se fall within the scope of either the DSA or the DMA. Similarly, the advertising-related provisions contained in those frameworks would not apply to them, even if they were to enter the advertising market in the future.⁷¹¹ Conversely, the Regulation on Political Advertising, which is not limited to platform services, would apply to such providers. Likewise, the GDPR remains fully applicable to their data processing activities. However, also in this context, the systemic risk management provisions included in the AI Act may considerably broaden the obligations of major providers in the near future.

Focusing on digital platforms, the open-ended nature of risk assessment provisions,⁷¹² the already demonstrated ineffectiveness of some implementation measures, such as the *pay-or-consent* model,⁷¹³ but also widespread allegations of non-compliance with the GDPR,⁷¹⁴ are all elements suggesting that the paradigm-shifting potential of recent regulations on the digital sector ultimately depends not only on the substantive rules but also on the enforcement architecture tasked with their application. The complex interplay between the various actors involved, including digital platforms, national authorities, European supervisory bodies, and courts, raises important questions regarding potential gaps or inefficiencies in oversight. Moreover, this chapter has contributed to show that the regulation of major players in the digital sector is dispersed across multiple legal instruments and therefore requires a holistic approach to implementation. The following chapter therefore examines in greater detail the enforcement structure governing digital

⁷¹¹ As widely expected, OpenAI has recently announced its entrance in the advertising market concerning ChatGPT: OpenAI (n 74).

⁷¹² Paul de Hert and Paweł Hajduk, 'EU Cross-Regime Enforcement, Redundancy and Interdependence. Addressing Overlap of Enforcement Structures in the Digital Sphere after Meta.' (2024) 2024 Technology and Regulation 291, 292 <<https://techreg.org/article/view/19322>> accessed 28 January 2025.

⁷¹³ Reportedly adopted by only 1% of users. See *supra*: Section 2.2.

⁷¹⁴ European Center for Digital Rights, 'GDPR: A Culture of Non-Compliance?' (noyb 2024) <https://noyb.eu/sites/default/files/2024-01/GDPR_a%20culture%20of%20non-compliance.pdf>.

regulations, with particular attention to the challenges related to coordination among the different frameworks and various actors involved.

V. AN HOLISTIC PERSPECTIVE ON DIGITAL PLATFORM REGULATION: CHALLENGES FOR EFFECTIVE OVERSIGHT AND ENFORCEMENT

As discussed in Chapter II, III, and IV, many of the new rules lack precision, and their actual scope will largely depend on how they are implemented and interpreted, both by platforms themselves and by oversight authorities. Risk management obligations are particularly relevant in this regard, as they require digital platforms to adopt appropriate measures without specifying what those measures should be. While this open-endedness allows the provisions to remain future-proof, adapting to technological advances and evolving societal risks, their practical scope is largely depending on the platforms' implementation choices and how public authorities evaluate those, creating a degree of legal uncertainty.

In light of these considerations, the enforcement framework of the provisions examined so far requires specific analysis. The importance of enforcement within the regulatory process has long been acknowledged, as it is essential to ensure that legal obligations effectively translate into compliance.⁷¹⁵ Throughout this chapter, enforcement is essentially understood as the activity through which competent administrative authorities monitor compliance and impose sanctions.⁷¹⁶ While various approaches exist for determining the optimal level of enforcement,⁷¹⁷ there

⁷¹⁵ Miroslava Scholten and Leander Stähler, 'Introduction to Research Handbook on the Enforcement of EU Law' *Research Handbook on the Enforcement of EU Law* (Edward Elgar Publishing 2023) 2 <<https://www.elgaronline.com/edcollchap/book/9781802208030/book-part-9781802208030-9.xml>> accessed 25 July 2025.

⁷¹⁶ John AE Vervaele, *Compliance and Enforcement of European Community Law* (Wolters Kluwer 1999) VII; Scholten and Stähler (n 715) 3.

⁷¹⁷ Robert Baldwin, Martin Cave and Martin Lodge, 'Enforcing Regulation' in Robert Baldwin, Martin Cave and Martin Lodge (eds), *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press 2011) 248 <<https://doi.org/10.1093/acprof:osobl/9780199576081.003.0011>> accessed 13 January 2026;

is a broad consensus that it must be effective in order to foster both special and general deterrence.⁷¹⁸ However, oversight of Big Tech have traditionally revealed structural shortcomings. In this respect, the Digital Services Act Package, encompassing both the DMA and the DSA, marked a significant step forward by placing greater emphasis on strengthening the enforcement architecture.

One of the key shortcomings addressed concerns the decentralised nature of previous enforcement models. Indeed, conferring enforcement in the hands of national authorities has often proved an inadequate approach, as Member States have frequently shown structural weaknesses when confronting major technological players,⁷¹⁹ lacking the expertise, capacity, and technical resources needed to effectively monitor compliance and take appropriate action.⁷²⁰ In addition, decentralised enforcement structures are vulnerable to interference with national political priorities.⁷²¹ Indeed, many EU regulations adopt the country-of-establishment principle, whereby the competent enforcement authority is located in the Member State where the service provider is established, regardless of where its services are offered. This has resulted in a high concentration of enforcement responsibilities within a small number of countries: among platforms designated as VLOPs and VLOSEs, ten are established in Ireland, four in the Netherlands, two in

Florentin Blanc and Michael G Faure, 'Smart Enforcement. Theory and Practice' (Social Science Research Network, 1 November 2018) <<https://papers.ssrn.com/abstract=3372956>> accessed 13 January 2026; S Shavell, 'The Optimal Structure of Law Enforcement' in Robert Baldwin, Colin Scott and Christopher Hood (eds), *A Reader on Regulation* (Oxford University Press 1998) <<https://doi.org/10.1093/acprof:oso/9780198765295.003.0011>> accessed 13 January 2026.

⁷¹⁸ Vervaele (n 716) VII.

⁷¹⁹ Hert and Hajduk (n 712) 297. See also this report from the European Union Agency for Fundamental Rights: European Union Agency for Fundamental Rights, 'GDPR in Practice – Experiences of Data Protection Authorities' <<https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities>> accessed 11 April 2025.

⁷²⁰ Filipe Brito Bastos and Przemysław Pałka, 'Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?' (2023) 19 European Constitutional Law Review 487, 489 <<https://www.cambridge.org/core/journals/european-constitutional-law-review/article/is-centralised-general-data-protection-regulation-enforcement-a-constitutional-necessity/65F232075D5ED87A1CE1E8F642E82206>> accessed 13 February 2025.

⁷²¹ Bastos and Pałka (n 720) 493.

Cyprus, two in Czechia, one in Germany, and one in Luxembourg. This geographical distribution largely reflects favourable tax regimes in those countries, but it can have significant spillover effects on the enforcement of digital regulations. Indeed, this situation not only requires these countries to devote substantial administrative resources to fulfil their supervisory duties, but may also create disincentives for strict enforcement, as national authorities may be reluctant to take action, fearing that it could undermine their jurisdiction's attractiveness to digital firms.

Unlike the GDPR, the PAR and the AVMS Directive which grant the Commission limited enforcement powers,⁷²² the Digital Services Package introduced a more centralised enforcement model. The DMA's enforcement, since it only applies to major platforms classified as 'gatekeepers', is completely centralised at the European Commission level. Conversely, under the DSA, the country-of-establishment principle is not fully abandoned but significantly mitigated for major platforms. Indeed, the Commission holds exclusive competence to designate VLOPs and VLOSEs and to enforce the special obligations applicable to them.⁷²³ However, these entities must also comply with the broader requirements for intermediary providers, hosting services, and platforms. For these broader requirements, enforcement is shared between the European Commission and national authorities (namely, the ones designated as Digital Services Coordinators), with the latter being competent only when the Commission has not initiated proceedings for the same infringement.⁷²⁴ In this regard, the preamble of the DSA

⁷²² Concerning GDPR enforcement, the powers conferred on the EC are very limited, mainly related to the ability to request opinions from the EDPB (see Articles 64(2), 68(5), and 70(1)). In the PAR, the EC has some coordination competences (e.g., Article 22(8)). Under the AVMSD, particularly regarding VSPs, the EC's competence is also primarily focused on coordination (see Articles 28a(6) and (7), 28b(9) and (10), and 29).

⁷²³ Article 56(2) of the DSA establishes the exclusive competence of the EC in the enforcement of the special obligations for VLOPs and VLOSEs included in the Section 5 of the DSA, Article 33 to 45.

⁷²⁴ DSA, Article 56(4).

justifies this shared competence by stating that the Commission is best placed to address systemic breaches of the DSA by major platforms, while national authorities are better suited to handle isolated infringements that do not raise systemic or cross-border concerns.⁷²⁵

The supervisory and enforcement role on major platforms comes with associated costs. To cover these, the Commission is empowered to impose an annual supervisory fee on designated VLOPs and VLOSEs,⁷²⁶ which is intended to offset the estimated expenses related to its supervisory tasks. Following an adversarial procedure, each provider receives an annual decision specifying the exact amount of the fee due. Individual amounts should take into account the expenses incurred by the Commission during the previous year and be proportional to the average number of monthly active users of each VLOP or VLOSE.⁷²⁷ The first of such decisions were issued in November 2023. Importantly, the Commission does not disclose the amount paid by each individual company; only the total annual sum collected is made public (approximately 45 million euros in 2023, and 58 million in 2024).

Apparently, some companies, such as Amazon and X, were exempted from paying the supervisory fee in the first year, as they had reported losses during the preceding financial year:⁷²⁸ while the decisions determining individual fees were challenged before the General Court by both Meta and TikTok.⁷²⁹ These decisions were

⁷²⁵ DSA, Recital 125.

⁷²⁶ DSA, Article 43.

⁷²⁷ DSA, Article 43(6). Specific methods to determine the amount of the fee have been outlined in a delegated regulation: Commission Delegated Regulation (EU) 2023/1127 of 2 March 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council with the detailed methodologies and procedures regarding the supervisory fees charged by the Commission on providers of very large online platforms and very large online search engines, C/2023/1257.

⁷²⁸ Foo Yun Chee, 'TikTok Challenges EU Supervisory Fee, Following Meta's Footsteps' *Reuters* (8 February 2024) <<https://www.reuters.com/technology/tiktok-challenges-eu-supervisory-fee-following-metas-footsteps-2024-02-08/>> accessed 4 March 2025.

⁷²⁹ CJEU, Case T-55/24, *Meta Platforms Ireland v Commission*, action brought on 5 February 2024; and Case T-58/24, *TikTok Technology v Commission*, action brought on 6 February 2024.

recently annulled on the grounds that the methodology for calculating the number of active users had been established through individual implementing decisions rather than a delegated act, as required by the DSA,⁷³⁰ leaving open the question of how the Commission will define the metric for future fee allocations; and whether this definition will align to the one used for designation purposes.⁷³¹

Centralisation is not the only critical point addressed by the Digital Services Package. A further challenge in enforcing obligations against large technology companies has traditionally lied in the significant information asymmetry, since the functioning of digital platforms is often opaque and not easily subject to external scrutiny. The DSA contains several provisions on this issue. First, it mandates VLOPs and VLOSEs to grant access to relevant data, upon a reasoned request, either to the competent Digital Services Coordinator (DSC) or to the European Commission, for the purpose of monitoring and assessing compliance with the DSA.⁷³² They must also provide explanations regarding the design, logic, functioning and testing of their algorithmic systems, including their recommender systems.⁷³³ Moreover, and this represents an important innovation, the DSA requires major platforms to grant data access to vetted researchers.⁷³⁴ The objective is to facilitate independent research into systemic risks and on the adequacy of the mitigation measures adopted. To qualify, researchers must first be granted the status of ‘vetted researchers’ by the competent DSC.⁷³⁵ This status depends on several

⁷³⁰ *Meta Platforms Ireland v Commission* [2025] Court of Justice of the European Union ECLI:EU:T:2025:842, T-55/24; *Tiktok Technology v Commission* [2025] Court of Justice of the European Union ECLI:EU:T:2025:843, T-58/24.

⁷³¹ See *supra*: Chapter II, Section 2.

⁷³² DSA, Article 40(1)(2).

⁷³³ DSA, Article 40(3).

⁷³⁴ DSA, Article 40(4).

⁷³⁵ Following Article 40(9) of the DSA, while the competence for granting this status pertains to the DSC of establishment of the service, researchers may also submit their application to the DSC of the Member State of the research organisation to which they are affiliated, which will conduct an initial assessment as to whether the respective researchers meet all of the required conditions. Subsequently, it will send the application, together with the initial assessment, to the competent DSC, who must take a decision without undue delay.

criteria, including affiliation with research organisation,⁷³⁶ independence from commercial interests, disclosure of funding sources, capacity to meet data security and confidentiality standards, proportionality of the data request, and commitment to making the research publicly accessible.⁷³⁷ Following the positive assessment of these criteria and a reasoned request by the competent DSC, platforms are legally obliged to provide such access. The DSA allows only two grounds for denying a request: either the platforms does not have access to the requested data, or granting access would pose significant risks to the security of the service or the protection of confidential information, particularly trade secrets.⁷³⁸ To operationalise this mechanism, the European Commission has recently adopted a delegated act defining procedures and requirements for data access applications, including the establishment of a centralised DSA data access portal.⁷³⁹

Under this framework, researchers are regarded as valuable ‘sparring partners’ for regulators: they can help define what constitutes a risk, investigate its root causes, and propose meaningful mitigation strategies.⁷⁴⁰ This approach reflects a broader trend toward diversifying oversight and enforcement mechanisms to enhance regulatory effectiveness in complex digital ecosystems – an approach which also includes the expansion of redress tools aimed at strengthening private

⁷³⁶ As defined in Article 2, point (1), of Directive (EU) 2019/790.

⁷³⁷ DSA, Article 40(8).

⁷³⁸ DSA, Article 40(5).

⁷³⁹ European Commission, ‘Delegated Act on Data Access under the Digital Services Act (DSA) | Shaping Europe’s Digital Future’ (*European Commission | Digital Strategy*, 2 July 2025) <<https://digital-strategy.ec.europa.eu/en/library/delegated-act-data-access-under-digital-services-act-dsa>> accessed 15 October 2025. Comments on the previous draft can be found in: John Albert, ‘Researcher Access to Platform Data: Experts Weigh in on the Delegated Act’ (*DSA Observatory*, 29 November 2024) <<https://dsa-observatory.eu/2024/11/29/researcher-access-to-platform-data-experts-weigh-in-on-the-delegated-act/>> accessed 21 May 2025; LK Seiling, Ulrike Klinger and Jakob Ohme, ‘Non-Public Data Access for Researchers: Challenges in the Draft Delegated Act of the Digital Services Act’ (*Tech Policy Press*, 5 December 2024) <<https://techpolicy.press/non-public-data-access-for-researchers-challenges-in-the-draft-delegated-act-of-the-digital-services-act>> accessed 21 May 2025.

⁷⁴⁰ Husovec, ‘Will the DSA Work? On Money and Effort’ (n 19) 27.

enforcement.⁷⁴¹ It also signals a paradigm shift: major platforms can no longer unilaterally decide which areas of their operations are open to research or which data they are willing to disclose.⁷⁴² Instead, access is now governed by a formal, legally binding process, with defined timeframes.

In parallel, VLOPs and VLOSEs are also required to make data available to independent auditors. Indeed, these platforms must undergo independent audits, at their own expense and at least once a year, to verify compliance with the obligations set out by the DSA, including any commitments made under codes of conduct or crisis protocols.⁷⁴³ As part of this process, auditors are entitled to access internal data and documentation, and to pose written or oral questions.⁷⁴⁴ The resulting audit reports can serve as a useful baseline for regulators in assessing whether major platforms are effectively reducing systemic risks. Although auditors are formally independent, they are still commissioned and paid by the companies they evaluate, potentially undermining objectivity and rigor of the audit process.⁷⁴⁵ However, the results of the first audit cycle revealed several points of non-compliance: with the sole exception of Wikipedia, every audited platform received a negative evaluation.⁷⁴⁶ Nonetheless, on average, companies were found to comply with more

⁷⁴¹ As further discussed below.

⁷⁴² Husovec, 'Will the DSA Work? On Money and Effort' (n 19) 28; Mathias Vermeulen, 'Researcher Access to Platform Data: European Developments' (2022) 1 *Journal of Online Trust and Safety* <<https://tsjournal.org/index.php/jots/article/view/84>> accessed 23 May 2025. Interestingly, obstructionism was shown by platforms in the past for publicly accessible data: Ryan Knutson, 'The Clash Between Facebook and Independent Researchers - WSJ Podcasts' *Wall Street Journal* (9 August 2021) <<https://www.wsj.com/podcasts/the-journal/the-clash-between-facebook-and-independent-researchers/8fda97fc-203d-4632-bc86-f81c0cbe5faf>> accessed 23 May 2025.

⁷⁴³ DSA, Article 37. The Commission also adopted a delegated act on independent audits: Commission Delegated Regulation (EU) 2024/436 of 20 October 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines, 2024/436.

⁷⁴⁴ DSA, Article 37(2).

⁷⁴⁵ Mark Scott, '5 Things to Know about the Digital Services Act's First Risk Assessments and Audits' (*Tech Policy Press*, 11 December 2024) <<https://techpolicy.press/5-things-to-know-about-the-digital-services-acts-first-risk-assessments-and-audits>> accessed 21 May 2025.

⁷⁴⁶ Scott (n 745).

than 85% of DSA requirements,⁷⁴⁷ giving reason to believe that full alignment may be within reach.⁷⁴⁸

In addition to this, VLOPs and VLOSEs must also establish an independent internal compliance function, structurally separate from their operational units, to oversee the effective implementation of regulatory duties.⁷⁴⁹ Provisions on external audits and internal compliance functions mirror similar obligations found in other legal sectors such as financial supervision, anti-money laundering, and data protection, where independent external audits and internal compliance bodies are standard practice. However, critics argue that these mechanisms often result in a little more than bureaucratic exercise, prioritising procedural compliance – or ‘box-ticking’ – over substantive improvements. Others raise concerns that the limited guidance provided by the DSA may shift regulatory power to these private actors, allowing them to shape the compliance landscape in ways that could ultimately empty the DSA’s objectives.⁷⁵⁰

To complete the overview on enforcement, it must be noted that, while this chapter primarily focuses on public enforcement, private enforcement has also been addressed by recent regulations, in recognition of its potential to promote compliance, particularly given that public authorities do not have the capacity to monitor all instances of non-compliance.⁷⁵¹ At the same time, the introduction of new remedies touches on one of the central challenges of the algorithmic society, namely access to justice against digital harms. Indeed, the DSA significantly expanded available remedies,⁷⁵² contributing to a globally improved access to

⁷⁴⁷ Scott (n 745).

⁷⁴⁸ Giovanni De Gregorio and Oreste Pollicino, ‘Auditing Platforms under the Digital Services Act’ [2024] *Verfassungsblog* <<https://verfassungsblog.de/dsa-auditors-content-moderation-platform-regulation/>> accessed 21 May 2025.

⁷⁴⁹ DSA, Article 41.

⁷⁵⁰ De Gregorio and Pollicino (n 748).

⁷⁵¹ Husovec, ‘Will the DSA Work? On Money and Effort’ (n 19) 31.

⁷⁵² De Gregorio and Demkova, ‘The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe’ (n 455).

justice.⁷⁵³ This includes mechanisms such as internal complaint systems and ODS bodies,⁷⁵⁴ as well as provisions aimed at strengthening judicial redress. Indeed, while judicial redress still largely depends on national legal systems, the DSA establish certain EU-level guarantees, including the right to compensation and the possibility for non-profit organisations to initiate class actions.⁷⁵⁵ Private enforcement before courts is mainly expected to occur in the country where the service is provided, assuming the claimant qualifies as a consumer. However, if the claimants do not qualify as a consumers, they may not be able to establish jurisdiction in their home court, potentially creating barriers to access to justice for business users.⁷⁵⁶ In addition to this, the Digital Services Act allows users and their representative associations to file complaints before the national Digital Services Coordinator, conferring on them a right to be heard and to receive information throughout the procedure.⁷⁵⁷

While the proliferation of private remedies has generally been views positively, it also raised concerns in academic literature, particularly regarding the risk of increased fragmentation and uncertainty around their access and functioning.⁷⁵⁸ More broadly, scholars have noted that the effectiveness of many DSA tools will heavily depend on the activation of social structures, such as consumer associations, communities of researchers, ODS, and trusted flaggers, whose degree of proactivity may significantly vary across local contexts.⁷⁵⁹ This question is connected with the broader role of individuals: only Europeans who are aware of their digital rights

⁷⁵³ Ortolani (n 20) 155; Kuczerawy (n 414) 169.

⁷⁵⁴ See *supra*: Chapter III, Section 1.2.

⁷⁵⁵ DSA, respectively Article 90 and 54.

⁷⁵⁶ Ortolani (n 20) 161.

⁷⁵⁷ DSA, Article 53.

⁷⁵⁸ De Gregorio and Demkova, 'The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe' (n 455).

⁷⁵⁹ Husovec, 'Will the DSA Work? On Money and Effort' (n 19) 23. With regard to vetted researchers, the success of this innovative mechanism will depend heavily on the availability of adequate funding.

will be able to properly enforce them.⁷⁶⁰ While the DSA provides single users with a broad range of transparency tools and procedural options, their impact will most likely depend on their use by expert intermediaries such as journalists and civil society organisations.⁷⁶¹

While all the innovations discussed above represent a promising step forward for the effective enforcement of the DSA, it must be noted that pre-existing enforcement structures, such as those established by the GDPR and the AVSMD, have not been amended. Moreover, the DSA lacks adequate coordination with other recent regulatory frameworks, such as the Regulation on Political Advertising and the Media Freedom Act. As a result, the overall legal framework has become increasingly complex and layered, both substantially and procedurally.

From a substantive perspective, coherence and coordination across the various legislative acts are not always evident, particularly given the widespread regulatory overlaps. Previous chapters have already illustrated this complexity. Chapter II and III showed how rules on liability and content moderation partially overlap with earlier frameworks, such as the AVSMD and the Copyright Directive, and are further complemented by more recent initiatives like the EMFA. Chapter IV revealed an additional layer of complexity, as rules on recommender systems intersect with data protection (notably the GDPR), but also with provisions included in the Digital Markets Act, the Regulation on Political Advertising, and the AI Act.

This regulatory fragmentation inevitably extends to enforcement, as each regulation is accompanied by its own dedicated enforcement architecture. The result is a system in which responsibilities are distributed across multiple national and supranational authorities, generating risks of redundancy, overlap and institutional conflicts. This concern had been shared by the European Data Protection Board

⁷⁶⁰ Husovec, ‘Will the DSA Work? On Money and Effort’ (n 19) 23.

⁷⁶¹ Husovec, ‘Will the DSA Work? On Money and Effort’ (n 19) 23.

before to the adoption of the Digital Services Package, particularly noticing the emergence of overlaps on data protection across the DSA, DMA and GDPR, resulting parallel supervisory structures.⁷⁶²

Concerns over what some have characterised as ‘regulatory brutality’⁷⁶³ have only recently begun to be acknowledged ‘politically’ at the EU level, for example by Commissioner Virkkunen,⁷⁶⁴ and have then led to simplification efforts, most notably through the proposal of a Digital Omnibus.⁷⁶⁵ However, such efforts have largely overlooked the complexities in the enforcement architecture, which is left fundamentally unchanged by the digital omnibus strategy.⁷⁶⁶ This growing awareness has also prompted European institutions and enforcement bodies to begin developing guidance on the intersections between different regulatory instruments, such as between the DSA and the GDPR,⁷⁶⁷ as well as between the DMA and the GDPR.⁷⁶⁸

⁷⁶² European Data Protection Board, ‘Statement on the Digital Services Package and Data Strategy’ <https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-digital-services-package-and-data-strategy_en> accessed 20 January 2025.

⁷⁶³ Vagelis Papakonstantinou and Paul De Hert, ‘The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of “Act-Ification”, “GDPR Mimesis” and “EU Law Brutality”’ (Social Science Research Network, 1 May 2022) <<https://papers.ssrn.com/abstract=4123313>> accessed 17 July 2025.

⁷⁶⁴ Toby Sterling, ‘EU Commission Looks to Cut Overlap in Tech Directives -Virkkunen’ *Reuters* (27 March 2025) <<https://www.reuters.com/technology/eu-commission-looks-cut-overlap-tech-directives-virkkunen-2025-03-27/>> accessed 11 April 2025.

⁷⁶⁵ Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus).

⁷⁶⁶ Giovanni De Gregorio and Simona Demkova, ‘Reordering the Enforcement of European Digital Regulation in Times on Omnibus’ *Enforcing the EU Digital Acquis* (Digicon 2025).

⁷⁶⁷ European Data Protection Board, ‘Interplay between the DSA and the GDPR: EDPB Adopts Guidelines’ (*European Data Protection Board*, 12 September 2025) <https://www.edpb.europa.eu/news/news/2025/interplay-between-dsa-and-gdpr-edpb-adopts-guidelines_en> accessed 15 September 2025.

⁷⁶⁸ European Commission, ‘Public Consultation on Joint Guidelines on the Interplay between DMA and GDPR’ (*European Commission | Digital Markets Act*, 9 October 2025) <https://digital-markets-act.ec.europa.eu/public-consultation-joint-guidelines-interplay-between-dma-and-gdpr-2025-10-09_en> accessed 11 October 2025.

Throughout this chapter, Section 1 examines examples of substantive overlaps among selected regulations in the digital sector. Section 2 then maps respective enforcement authorities, illustrating how the proliferation of enforcement bodies creates a fragmented landscape that gives rise to enforcement overlaps potentially undermining the effective application of the DSA and its complementary regulations.

1. TECHNOLOGICAL INTERSECTIONS AND REGULATORY OVERLAPS

As digital services and functionalities often operate interdependently, it is almost inevitable for online platforms to fall under multiple classifications and, therefore, being simultaneously subject to various legal frameworks. The regulation of platforms indeed intersects with data protection, media regulations, artificial intelligence, competition and consumer protection.

The overlap between rules on online content and data protection is particularly evident given how online platforms generally operate.⁷⁶⁹ As it is well-known, data collection lies at the core of platforms' business model,⁷⁷⁰ feeding the algorithms that determine how content is disseminated. For this reason, the DSA imposes restrictions on the use of personal data for targeted content recommendations,⁷⁷¹ especially regarding online advertisement. In doing so, the regulation refers repeatedly to the GDPR. As illustrated above,⁷⁷² Article 26 of the DSA refers to the definition of 'special categories of data' given by Article 9 of the GDPR. However, while the GDPR restricts the processing of such 'sensitive' data to specific cases, the DSA goes further by completely prohibiting the profiling of users based on this data for online advertisement purposes. The interplay among these two frameworks has made be object of the recent guidelines issued by the EDPB, also addressing

⁷⁶⁹ De Gregorio (n 165) 131.

⁷⁷⁰ See *supra*: Chapter I and IV.

⁷⁷¹ See DSA, Article 26 and 28.

⁷⁷² See *supra*: Chapter IV, Section 1.2.

the question of cross-regulatory cooperation between authorities to coordinate enforcement.⁷⁷³

Beyond the DSA, online advertising is also subject to consumer protection laws⁷⁷⁴ and the PAR. Indeed, when the advertisement is ‘political’,⁷⁷⁵ the PAR introduces further obligations related to transparency and data use, complementing the requirements set by the DSA and other data protection regulations. More precisely, the Regulation requires online intermediaries to obtain explicit user consent for targeting political advertising, and to provide an option for users to access their services without giving such consent.⁷⁷⁶ Finally, similarly to the DSA, it completely prohibits targeted political advertisement based on profiling using special categories of data, as defined by Article 9 of the GDPR.⁷⁷⁷

Additional restrictions on the use of data are introduced by the Digital Markets Act, which prohibits gatekeepers from combining users’ data across different services without explicit consent,⁷⁷⁸ a practice that may also be unlawful under the GDPR if lacking a legitimate basis under Article 6.⁷⁷⁹ In this context, as mentioned above, the European Commission and the EDPB are currently elaborating guidelines on the intersection between the DMA and the GDPR.⁷⁸⁰ Furthermore, data combination practices can also be deemed anti-competitive under EU competition

⁷⁷³ European Data Protection Board, ‘Interplay between the DSA and the GDPR: EDPB Adopts Guidelines’ (n 767).

⁷⁷⁴ For instance, advertisement is regulated by the Unfair Commercial Practices Directive (Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council).

⁷⁷⁵ As defined by PAR, Article 3(2). See *supra*: Chapter IV, Section 3.1.

⁷⁷⁶ PAR, Article 18. See *supra*: Chapter IV, Section 3.2.

⁷⁷⁷ PAR, Article 18. See *supra*: Chapter IV, Section 3.2.

⁷⁷⁸ DMA, Article 5(2). See *supra*: Chapter IV, Section 2.2.

⁷⁷⁹ GDPR, Article 6.

⁷⁸⁰ European Commission, ‘Public Consultation on Joint Guidelines on the Interplay between DMA and GDPR’ (n 768).

law, as demonstrated by the *Meta Platforms* case,⁷⁸¹ which originated from the German Federal Cartel Office's findings that the combination of user data from different sources was both a breach of the GDPR and an abuse of dominant position.⁷⁸²

Further complexity arises from the intersection between the DSA and the Audiovisual Media Services Directive. This directive, which was not amended by the DSA, required Member States to impose stringent obligations on Video-Sharing Platforms (VSPs) to prevent the spread of certain harmful content, including illegal content, terrorism, and incitement to violence or hatred against groups or individuals.⁷⁸³ A similar need to mitigate risks related to the spread of harmful content is also contained in the DSA,⁷⁸⁴ applicable to online platforms which qualify as VLOPs or VLOSEs.⁷⁸⁵ Additionally, particular emphasis is placed by the AVSMD on the protection of minors, a concern also addressed by the DSA.⁷⁸⁶ As a result, if a VLOP also qualifies as VSP, as it is the case for YouTube, it must comply with both sets of rules.

Moreover, the European Media Freedom Act,⁷⁸⁷ particularly Article 18, complements the safeguards established by the DSA for users subjected to content restrictions, providing additional protections when the affected user is a media service provider.⁷⁸⁸ More precisely, while the DSA requires online platforms to

⁷⁸¹ CJEU, *Meta platforms and Others* (n 632).

⁷⁸² See *supra*: Chapter IV, Section 2.2.

⁷⁸³ AVMS Directive, Article 28b. See *supra*: Chapter 0, Section 1.3.

⁷⁸⁴ DSA, Articles 34 and 35. See *supra*: Chapter 0, Section 2.4.

⁷⁸⁵ As defined by Article 33 of the DSA and following the designation made by the European Commission. See *supra*: Chapter 0, Section 2.1.

⁷⁸⁶ DSA, Article 28.

⁷⁸⁷ Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a Common Framework for Media Services in the Internal Market and amending Directive 2010/13/EU (European Media Freedom Act).

⁷⁸⁸ See *supra*: Chapter 0, Section 2.2.

issue a statement of reasons⁷⁸⁹ and provide redress mechanisms⁷⁹⁰ for users whose content has been restricted,⁷⁹¹ the EMFA mandates prior notification before any restriction is imposed and grants priority treatment for complaints related to content moderation when the affected party is a media service provider on VLOPs.⁷⁹² The EMFA contains, however, some explicit coordination rules with the DSA, for instance, when establishing that compliance with Article 18 EMFA may be taken into consideration by the European Commission when enforcing the DSA.⁷⁹³

Likewise, the AI Act may also be relevant to online platforms, provided that they can operate both as AI providers and deployers.⁷⁹⁴ As a result, the AI Act presents several potential overlaps with the DSA. For instance, providers of generative AI models with systemic risk⁷⁹⁵ bear certain risk-management obligations.⁷⁹⁶ If a VLOP or VLOSE also fall into this category, it could be required to conduct a systemic risk assessment and mitigation under both regulations. This possibility is explicitly taken into consideration by the AI Act's preamble, which states that to the extent that AI systems or AI models are embedded within designated VLOPs and VLOSEs, they are subject to the risk assessment framework of the DSA.⁷⁹⁷ Consequently, the risk-management provisions of the AI Act should be considered

⁷⁸⁹ DSA, Article 14. More precisely, this provision is applicable to all hosting providers, not only to online platforms.

⁷⁹⁰ DSA, Article 20. This provision is only applicable to online platforms.

⁷⁹¹ Content restrictions are defined by the above-mentioned Article 14 of the DSA.

⁷⁹² Media services are defined by Article 2 of the EMFA.

⁷⁹³ Recital 55 EMFA states that, for enforcing the DSA, the Commission can consider the opinions submitted by the European Board of Media Services on the outcomes of the 'meaningful dialogue' VLOPs and media service providers can initiate in order to find an amicable solution for terminating unjustified restrictions (See: EMFA, Article 19). Furthermore, Recital 56 states that the outcomes of such dialogues may be taken into account by the Commission when supervising systemic risks assessment under Article 34 and 35 of the DSA.

⁷⁹⁴ One may also question whether generative AI systems should fall *per se* within the definition of online platforms under the DSA. This does not appear to be the position of EU lawmakers, who states that AI systems *may* be provided as intermediary services, thereby triggering the application of the DSA (AI Act, Recital 119).

⁷⁹⁵ Those identified in line with AI Act, Article 51.

⁷⁹⁶ AI Act, Article 55(1).

⁷⁹⁷ As explicitly recognized by the AI Act itself at Recital 118.

‘automatically’ fulfilled, unless distinct systemic risks specifically related to AI models emerge and are identified.⁷⁹⁸ Another connection between the AI Act and the DSA arises in relation to the obligations placed on AI providers and deployers to enable the detection and disclosure of artificially generated or manipulated outputs,⁷⁹⁹ which is explicitly recognised as relevant to addressing the risks on democratic processes, civic debates, and electoral integrity, as outlined in Article 34 of the DSA.⁸⁰⁰ While these regulatory connections can be considered a positive step toward a more integrated framework, no corresponding coordination exists in the enforcement structure.

Instead, as examined in the next section, the enforcement structures of these regulations have not adequately considered their substantive regulatory overlaps, with competencies and responsibilities which are spread across multiple national and supranational authorities. In some cases, these authorities operate under the same legal bases (*intra-framework*), while in others, their mandates arise from layered regulatory frameworks (*cross-framework*). The next sections explore overlapping competencies at the national level, both within single member states and in transnational cases, before delving into the structure of supranational enforcement.

2. THE FRAGMENTED ENFORCEMENT STRUCTURE OF PLATFORM REGULATION

The expansion of the EU digital acquis⁸⁰¹ has been accompanied by a proliferation of authorities with competence in the digital sector, as each regulatory system

⁷⁹⁸ AI Act, Article 55.

⁷⁹⁹ AI Act, Article 50.

⁸⁰⁰ AI Act, Recital 120.

⁸⁰¹ Scholars have increasingly started to refer to the growing body of legislation in the digital sector as the EU digital acquis. See: Giovanni De Gregorio and Simona Demkova, *Enforcing the EU Digital Acquis* (Digicon 2025); Artur Bogucki and others, ‘The AI Act and Emerging EU Digital Acquis’ (CEPS 2022) <<https://www.ceps.eu/ceps-publications/the-ai-act-and-emerging-eu-digital-acquis/>> accessed 13 January 2026; Irene Kamara and Marco Bassini, ‘The Cybersecurity and AI

typically establishes its own governance and enforcement apparatus. The consequence is not merely bureaucratic expansion: the intertwinement among different regulatory regimes applying to online platforms can create enforcement overlaps and potential clashes when multiple regulators claim a role over the same issue. The dispersion of responsibilities across various actors can therefore lead to inefficiencies and conflicting decisions. While overlap may be viewed positively in some respects, allowing for a plurality of perspectives and values to be considered, it also carries significant risks. The fragmentation of responsibilities can weaken enforcement efforts and create an unpredictable environment for economic operators.⁸⁰² Moreover, although not every instance of overlap results in conflict, such an outcome remains a possibility when authorities fail to coordinate or to reach an agreement.

The following table provides a sample of the bodies broadly vested with enforcement powers or consultative role for a selected set of regulations on digital services, using two Member States as examples (Italy and Ireland).

Table 2. Overview of EU national and supranational authorities involved in the enforcement of selected regulations

		DSA	DMA	AI ACT	GDPR	PAR	EMFA	AVMS	COMP	CONS
EU	European Commission	✓	✓	✓					✓	
	European Board for Media Services						✓	✓		
	European Data Protection Board				✓					

Nexus in the EU Digital Acquis' [2025] MediaLaws <<https://www.medialaws.eu/rivista/the-cybersecurity-and-ai-nexus-in-the-eu-digital-acquis/>> accessed 13 January 2026.

⁸⁰² Main advantages and disadvantages of regulatory overlap are analysed in: Lachlan Robb, Trent Candy and Felicity Deane, 'Regulatory Overlap: A Systematic Quantitative Literature Review' [2022] Regulation & Governance - Wiley Online Library <<https://onlinelibrary.wiley.com/doi/10.1111/rego.12504>> accessed 5 June 2025.

	European Competition Network					✓	
	European AI Board	✓					
	Consumer Protection Cooperation Network						✓
	European Board for Digital Services	✓					
IT	Media regulatory authority (AGCOM)	✓			✓	✓	✓
	Data Protection Authority (Garante)			✓	✓		
	National competition authority (AGCM)					✓	✓
	National Cybersecurity Agency			✓			
	AgID			✓			
IE	Broadcasting Authority (BCI)					✓	
	Media Commission (Comisiún na Meán)	✓			✓	✓	
	Data Protection Authority			✓	✓		
	Competition and Consumer Protection Commission (CCPC)	✓				✓	✓
	AI Act supervisory			✓			

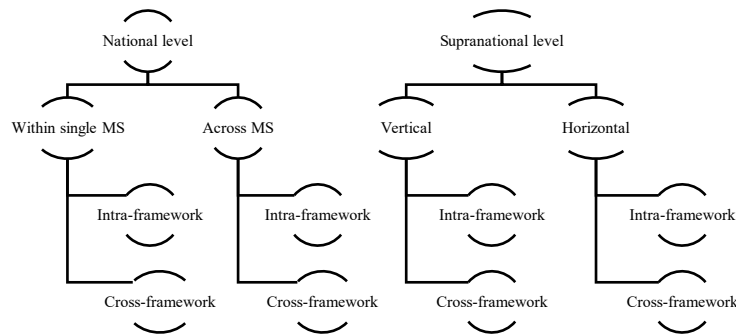
	authorities (still unclear)
+ 25 MS	[...]

This institutional proliferation occurs at the national and supranational levels, creating both vertical and horizontal overlaps under the same regulatory framework (intra-framework) or across different ones (cross-framework). Enforcement at the national level presents several potential overlaps, as multiple authorities may become involved in the same case, either within a single Member State or across different Member States. In addition, several EU regulations establish a supranational layer of enforcement, creating space for vertical overlaps between national and supranational bodies, as well as horizontal overlaps among different supranational institutions.

To facilitate the analysis of enforcement overlaps, this section is structured according to different criteria: the level at which the overlap arises (national or supranational), the geographic scope (within a single Member State or across Member States), the institutional relationship (vertical or horizontal),⁸⁰³ and the relevant regulatory scope (distinguishing between intra-framework and cross-framework overlaps). This classification is visually summarised in the following table.

⁸⁰³ Overlaps at the national level are, by definition, horizontal, as they occur between authorities operating at the same institutional level within a Member State.

Table 3. Types of overlaps between competent authorities



The analysis will proceed in three parts: the first part will focus on national-level enforcement (2.1), the second will focus on transnational coordination (2.2), and the third on supranational enforcement involving EU-level institutions (2.3). As already mentioned, this chapter does not address private enforcement; however, it is important to recall that national courts are also competent to apply digital regulations, adding another layer of potential divergent interpretations and conflicting decisions.

2.1. NATIONAL AUTHORITIES ENFORCING REGULATIONS ON DIGITAL PLATFORMS

Enforcement at the national presents severe fragmentation, and multiple authorities can find themselves involved in the same case. This situation can arise either under the same regulatory framework, or under different ones, as illustrated below.

Multiple national authorities enforcing the same regulation

Within a single Member State, various authorities may be assigned with enforcement responsibilities under the same regulatory framework (*intra-framework*). This multiplication results either from the rules directly established by the EU or from the discretion left to Member States regarding the enforcement structure. EU regulations often leave Member States discretion in deciding how

many authorities to designate for the supervision of a given regulation, even if some form of national coordination is normally required. This is the case under the DSA, which nevertheless requires Member States to appoint a single Digital Services Coordinator.⁸⁰⁴ A similar structure applies to the GDPR,⁸⁰⁵ which also requires the designation of a single Data Protection Authority, mandated to participate in the European Data Protection Board. In both cases, enforcement at national level may therefore involve one or more competent authorities. By contrast, some EU regulations expressly provide for multiple supervisory authorities. The Regulation on Political Advertisement is a prominent example, as it assigns oversight responsibilities to different authorities depending on the specific provisions and entities at stake. More precisely, supervision of rules on targeted online political advertisement falls under the competence of the national Data Protection Authority, while for other provisions, Member States are required to designate one or more competent authorities (e.g., those responsible consumer protection or audio-visual services).⁸⁰⁶ Moreover, the Digital Services Coordinator⁸⁰⁷ is responsible for coordinating enforcement concerning online intermediaries, including online platforms which fall into the category of VLOP and VLOSE.⁸⁰⁸ As a result, enforcing the PAR at national level involves at least two different authorities, namely, the DPA and the DSC, but may also require the involvement of three or more, including the competition and media authorities, depending on national institutional arrangements. However, coordination should be facilitated by the requirement for Member States to designate a single national contact point.⁸⁰⁹

Multiple national authorities enforcing overlapping regulations

⁸⁰⁴ DSA, Article 49(1)(2).

⁸⁰⁵ GDPR, Article 51(1).

⁸⁰⁶ PAR, Article 22(1)(3)(4).

⁸⁰⁷ Designated in line with Article 49(2) of the DSA.

⁸⁰⁸ PAR, Article 22(1)(3)(4).

⁸⁰⁹ PAR, Article 22(9).

Wider fragmentation emerges when examining overlaps across different regulatory frameworks and their respective national supervisory authorities (*cross-framework*). At the national level, the DSA is (primarily) enforced by the Digital Services Coordinator, while the GDPR falls (primarily) under the competence of the DPA. Additionally, the enforcement of the PAR is divided among the DPA, the DSC and another potential authority (e.g., those responsible consumer protection or audio-visual services). Moreover, the AVMS Directive assigns responsibilities to an Authority for Audiovisual Services, the Media Freedom Act is supervised by the national media regulators but can be taken into consideration by the DSC when applying the DSA, and the AI Act requires the designation of additional national authorities. Finally, National Competition Authorities (NCAs) remain competent in cases related to digital markets and unfair competition, while multiple authorities with a competence in consumer protection can be present.

However, the level of actual enforcement fragmentation varies significantly across Member States.⁸¹⁰ In some countries, the communications authority operates both under the DSA and the AVSM directive, with the NCA also handles consumer protection and is possibly designated under the PAR. However, enforcement structures can be further centralised or decentralised, depending on the national

⁸¹⁰ An example of this asymmetric enforcement structure is the designation of the DSCs. Out of twenty-seven Member States, twenty-one have chosen as DSC the national authority for communications or media. However, in eleven of these cases, the DSC is different from the AVMS authority, while in one (Estonia), the communications authority also holds consumer protection competence. Among the remaining six Member States, two have not designated their DSC yet, two have designated the competition and consumer protection authority, one has assigned the role to a consumer protection authority (separate from its National Competition Authority), and another has designated the competition authority, which – conversely – does not oversee consumer protection). This situation can create several frictions. First, transnational cases could involve – for instance – two authorities from one Member State and three from another, each with different roles and competences. Additionally, national cooperation frameworks among authorities may significantly differ. For instance, a DSC may be required to consult other authorities, while another DSC may not face the same obligation. See: Anna Vicinanza, ‘Asymmetric National Enforcement Structures for EU Digital Rules: Can Cross-Border and Cross-Sector Cooperation Work?’ in Simona Demkova and Giovanni De Gregorio, *Enforcing the EU Digital Acquis* (The Digital Constitutionalist 2025) <<https://digi-con.org/enforcing-the-eu-digital-acquis/>> accessed 10 February 2026.

framework. In Spain, for instance, the *Comisión Nacional de los Mercados y la Competencia* (CNMC) is responsible for enforcing the DSA, the AVSM Directive, and competition law, resulting in a relatively centralised system. In contrast, federal countries like Germany and Belgium have a markedly fragmented system, as AVSM supervisory authorities are designated at the federated state level.

The result of the fragmentation existing in certain Member States is that conflicts among national authorities in enforcing different regulations on digital platforms may arise easily, particularly when a platform's conduct is deemed violating multiple regulatory frameworks simultaneously. One example of potential conflict is the above-mentioned *Meta Platforms* case, which required coordination between the German Data Protection Authority and Competition Authority.⁸¹¹ Additional examples of conflicts among different national authorities can be found in Italy. In one case, the national consumer protection authority sanctioned Meta for unfair commercial practices, including its failure to provide exhaustive explanation for service interruptions. However, the national DSC viewed this conduct as a violation of the DSA and asserted jurisdiction over the matter.⁸¹² A comparable case involved TikTok, which was sanctioned by the national consumer protection authority for the algorithmic dissemination of harmful content among minors, creating addiction and impacting consumers' self-determination. The national DSC considered again this issue to fall within its jurisdiction under the DSA.⁸¹³ This case suggests that the conflicting authority (i.e., the DSC) could also initiate proceedings for the same

⁸¹¹ CJEU, *Meta platforms and Others* (n 632).

⁸¹² Autorità Garante delle Comunicazioni, 'Delibera 110/24/CONS. Richiesta Di Parere Dell'Autorità Garante Della Concorrenza e Del Mercato in Merito al Procedimento Avviato Nei Confronti Di Meta Platforms Inc. e Meta Platforms Ireland Limited in Materia Di Pratiche Commerciali Scorrette PS/12566.' <<https://www.agcom.it/provvedimenti/delibera-110-24-cons-0>>.

⁸¹³ Autorità Garante delle Comunicazioni, 'Delibera 325/23/CONS. Richiesta Di Parere Dell'Autorità Garante Della Concorrenza e Del Mercato in Merito al Procedimento Avviato Nei Confronti Di Tik Tok Italy S.r.l. in Materia Di Pratiche Commerciali Scorrette PS/12543' <<https://www.agcom.it/provvedimenti/delibera-325-23-cons>>.

conduct, potentially exposing the platform to double sanctions, and create conflicting decisions.

Table 4. Types of overlaps within a single Member State

<i>Enforcement within a single Member State</i>	
<i>Intra-framework Overlaps</i>	Multiple national authorities competent under the same legal regime
<i>Example</i>	DPA vs DSC both designated for enforcing the PAR in the same MS
<i>Cross-framework Overlaps</i>	Multiple national authorities competent under different legal regimes
<i>Example</i>	National DPA vs National NCA

2.2. TRANSNATIONAL COORDINATION IN A FRAGMENTED ENFORCEMENT LANDSCAPE

Beyond overlaps within individual Member States, the cross-border activity of digital services introduces another layer of potentially conflicting enforcement, as multiple authorities from different Member States may claim competence over the same issue. Such overlaps can arise both when authorities seek to apply the same regulation (i.e., intra-framework conflicts across Member States), or when they invoke different legal frameworks (i.e., cross-framework conflicts across Member States).

Transnational enforcement under a single framework

Most of the regulations examined establish clear criteria for determining the competent national authority in cross-border cases, often based on the country-of-establishment principle. Under the DSA, the Member State in which the main establishment of the intermediary provider is located holds exclusive supervisory and enforcement competence, except for powers explicitly granted to the European

Commission.⁸¹⁴ The country-of-establishment rule also applies to the oversight of Video-Sharing Platforms under the AVMSD,⁸¹⁵ and to the PAR.⁸¹⁶ Similarly, under the GDPR, when data processing occurs across multiple jurisdictions, the *one-stop-shop* mechanism ensures that the DPA of the country where the data processor's main establishment is located assumes a leading role in enforcement.⁸¹⁷ However, not all regulations affecting online platforms follow the country-of-establishment principle. For instance, under competition law and consumer protection regulations, the mere provision of services within the territory of a Member State is sufficient to establish the competence of that Member State's relevant authority, regardless of where the provider is based.

To facilitate enforcement in transnational cases, many of the examined regulations also contain rules framing cooperation among national authorities and have established supranational networks to serve as *fora* for coordination. This is the case for the European Board for Digital Services established by the DSA (EBDS); the European Data Protection Board for GDPR (EDPB); the European Regulators Group for Audiovisual Media Services (ERGA) for AVSMD, now replaced by the European Board for Media Services (EBMS);⁸¹⁸ the Consumer Protection Cooperation Network (CPC), the European Competition Network and the European Artificial Intelligence Board (EAIB). For the PAR, a European network for national contact points is expected.⁸¹⁹

While these explicit coordination mechanisms facilitate enforcement in transnational cases under the same regulation (*intra-framework*), *cross-framework* coordination remains a significant challenge.

⁸¹⁴ DSA, Article 56(1).

⁸¹⁵ AVSMD, Article 28a.

⁸¹⁶ PAR, Article 22.

⁸¹⁷ GDPR, Article 56.

⁸¹⁸ EMFA, Article 8.

⁸¹⁹ Regulation on Political Advertisement, Recital 101.

Transnational enforcement from a cross-framework perspective

While individual regulations on digital platforms provide mechanisms to streamline cross-border enforcement, no equivalent transnational coordination system exists when multiple regulatory frameworks apply concurrently. Once again, this issue stems from substantive overlaps between legal instruments, particularly when the same conduct is subject to multiple, partially overlapping sets of rules.

The situation becomes even more complex when overlapping regulatory frameworks apply different criteria for determining jurisdiction in cross-border cases. The authority competent to enforce the GDPR under the *one-stop-shop* mechanism may fall under the jurisdiction of a different Member States than the authority competent under other frameworks, such as consumer protection, even when addressing the same underlying conduct. In the above-mentioned *Meta platforms* case, the German Competition Authority and the Irish Data Protection Authority could both have claimed competence, the former based on the country where the service is provided, and the latter based on the country of establishment.

The types of overlaps described in this section can lead to conflicts in transnational enforcement, as summarised in Table 5.

Table 5. Types of overlaps across Member States

Transnational Enforcement	
<i>Intra-framework Overlaps</i>	Multiple authorities competent under the same legal regime across Member State
<i>Example</i>	A DPA in one Member State vs a DPA in another Member State
<i>Cross-framework Overlaps</i>	Multiple authorities competent under different legal regimes across Member State
<i>Example</i>	A DPA in one Member State vs a NCA in another Member State

This situation at the national level does not exhaust the challenges in enforcing the EU digital acquis. Indeed, it is further compounded by inconsistencies at the supranational level, leading to vertical and horizontal overlaps.

2.3. SUPRANATIONAL ENFORCEMENT OF DIGITAL PLATFORMS REGULATIONS

The supranational enforcement structure not only mirrors many of the challenges seen at the national level but also increases fragmentation. The existence of an EU governance layer introduces both horizontal and vertical overlaps. Horizontal tensions concern coordination among different EU bodies, while vertical ones arise between national and supranational authorities. As with national enforcement, intra-framework coordination among different competent authorities is organised through regulation from the Union. In contrast, cross-framework enforcement reveals several inconsistencies, particularly because some regulations adopt a more centralised approach, while others primarily grant power to national authorities, thereby increasing the risk of vertical conflicts.

It must be noted that supranational enforcement is not limited to the European Commission but also includes supranational regulatory networks, increasing the potential for both vertical and horizontal conflicts to arise. As already mentioned in the previous section, most of the regulations that have been examined establish supranational networks and bodies, whose powers and role, however, may vary significantly. Some of these bodies primarily serve advisory and coordination functions, ensuring consistency across enforcement actions but without binding authority. This includes the European Board for Digital Services under the DSA,⁸²⁰ and the network of national contact points established under the PAR.⁸²¹ Others, however, hold stronger enforcement powers, including the ability to adopt binding opinions and resolve conflicts between national authorities. This is the case for the

⁸²⁰ A list of the functions of the Board can be found in Article 63 of the DSA.

⁸²¹ Its role is presented in Article 22(8) of the Regulation on Political Advertisement.

European Data Protection Board and, to some extent, the European Board for Media Services, which substituted the ERGA.⁸²²

Vertical relationships in the enforcement structure

The existence of a European-level layer of enforcement raises the issue of coordinating national and supranational authorities, i.e. regarding the management of vertical relationships. These relationships can both emerge under the same regulatory frameworks, or across different frameworks, particularly in cases involving substantive regulatory overlaps.

Vertical relationships under a single framework

The expansion of the European regulatory intervention has led an increasing supervisory role of the European Commission, whose powers vary significantly depending on the regulatory framework in question. Unlike, the GDPR, the PAR and the AVMS Directive which grant the Commission limited enforcement powers,⁸²³ the adoption of the Digital Services Package, which includes both the Digital Markets Act and the Digital Services Act, marked a shift toward a more centralised enforcement structure compared to other regulations. As mentioned above, the DMA's enforcement is completely centralised at the European Commission level. Conversely, under the DSA the European Commission holds exclusive competence for designating VLOPs and VLOSEs⁸²⁴ and enforce the special obligations applicable to them.⁸²⁵ However, VLOPs and VLOSEs must also comply with the broader requirements for intermediary providers, hosting services,

⁸²² A list of the functions of the EBMS can be found in Article 13 of the EMFA. The main functions of the EDPB are listed in Articles 70, 64 and 65 of the GDPR.

⁸²³ Concerning GDPR enforcement, the powers conferred on the EC are very limited, mainly related to the ability to request opinions from the EDPB (see Articles 64(2), 68(5), and 70(1)). In the PAR, the EC has some coordination competences (e.g., Article 22(8)). Under the AVMSD, particularly regarding VSPs, the EC's competence is also primarily focused on coordination (see Articles 28a(6) and (7), 28b(9) and (10), and 29).

⁸²⁴ As defined by DSA, Article 33.

⁸²⁵ Article 56(2) of the DSA establishes the exclusive competence of the EC in the enforcement of the special obligations for VLOPs and VLOSEs included in the Section 5 of the DSA, Article 33 to 45.

and platforms. For these broader requirements, enforcement is shared between the European Commission and national authorities, with a pre-emption mechanism in favour of the former.⁸²⁶ From an intra-framework perspective, therefore, although both national authorities and the Commission may, in theory, initiate proceedings concerning the same case, the DSA establishes a clear criterion for the vertical allocation of enforcement powers.

A notable example of vertical conflicts arose in the context of GDPR enforcement. In a case regarding online targeted advertising, the adoption of a binding opinion by the EDPB based on the request of the Irish Data Protection Commission has led to a vertical conflict.⁸²⁷ Indeed, the Irish authority went before the EU General court, claiming the EDPB had exceeded its powers, undermining the autonomy of the Irish DPA. However, the General Court dismissed the case underlining how the power of the EDPB to adopt binding opinions directly results from the GDPR, as a mechanism to ensure its consistent application across Member States.⁸²⁸ As such, the GDPR, like the DSA, sets out clear rules for managing vertical relations between national and supranational authorities responsible for its enforcement.

Vertical relationships from a cross-framework perspective

From a cross-framework perspective, the overlap between centralised and decentralised regulatory frameworks creates significant enforcement challenges. An example is represented by the interaction between the DSA and the GDPR. While the GDPR grants national data protection authorities the primary responsibility for enforcing data protection rules, the DSA introduces additional obligations related to online advertising transparency and data processing which in

⁸²⁶ DSA, Article 56(4). Recital 125 justifies the share competence considering that the EC is in a better position to address systemic violations of general DSA's provisions by major platforms, while national authorities could be better placed to address individual infringements that do not raise any systemic or cross-border issues.

⁸²⁷ European Data Protection Board, 'Binding Decision 3/2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and Its Facebook Service (Art. 65 GDPR)'.

⁸²⁸ *Data Protection Commission v European Data Protection Board* [2025] Court of Justice of the European Union ECLI:EU:T:2025:116, T-70/23, T-84/23 and T-111/23.

the case of VLOPs and VLOSEs are enforced by the European Commission.⁸²⁹ This dual regulatory structure can lead to overlapping competences, where both the European and national authorities must coordinate their approaches to ensure consistent enforcement.

The same tension exists in the relationship between the centralised enforcement towards VLOPs and VLOSEs under the DSA and the decentralised enforcement structure in the field of consumer protection. This has become particularly evident regarding proceedings against the marketplace Temu, which has been subject to investigations initiated both by the European Commission and by national consumer protection authorities.⁸³⁰ Temu was designated as a Very Large Online Platform on 31 May 2024, thereby allowing the European Commission to act under the DSA, particularly with regard to obligations related to systemic risks, transparency of recommender systems, and data access for researcher. In parallel, consumer protection authorities investigated under the consumer protection acquis, pursuing concerns such as misleading advertising and the sale of unsafe products. In this context, both a coordinated action lead by the CPC Network and individual actions launched by single national authorities have been reported.⁸³¹ The European Commission clarified that the CPC Network's coordinated action against Temu is without prejudice to ongoing proceedings initiated by other national authorities. Moreover, all proceedings under consumer law are without prejudice to any action

⁸²⁹ A similar comparison can be drawn between the fully centralised DMA and the decentralised structure of the GDPR (see below on the 'pay-or-consent' model and the EDPB Opinion). By contrast, the case of competition law is peculiar: Articles 101 and 102 of the TFEU are enforced through a parallel structure, allowing both the European Commission and National Competition Authorities to act. However, Regulation 1/2003, Article 11, establishes a coordination mechanism, requiring NCAs to inform the Commission about ongoing cases, while granting the Commission the power to assume competence when deemed necessary. This means that in the absence of an intervention by the Commission, NCAs remain fully competent.

⁸³⁰ European Commission, 'Commission and national authorities urge Temu to respect EU consumer protection laws' (*European Commission*, 8 November 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5707> accessed 16 April 2025.

⁸³¹ European Commission, 'Commission and national authorities urge Temu to respect EU consumer protection laws' (n 830)..

that the European Commission may initiate under the DSA. While the Commission is coordinating with the CPC Network, individual national authorities appear to be excluded from this dialogue, potentially leading to duplication of sanctions and conflicting decisions.

The types of overlaps at the supranational level presented in this section can lead to various vertical conflicts in the enforcement of the EU digital acquis, as summarised in Table 6.

Table 6. Types of overlaps conflicts at the supranational level

<i>Vertical Relationships</i>	
<i>Intra-framework Overlaps</i>	EU and national authorities competent under the same legal regime
<i>Example</i>	EU Commission vs DSC or EDPB vs DPA
<i>Cross-framework Overlaps</i>	EU and national authorities competent under different legal regimes
<i>Example</i>	EU Commission vs national Consumer protection authorities

In addition to these types of vertical conflicts, coordination issues may arise among different supranational networks or between the Commission and a sectoral network, particularly when their respective mandates overlap. These types of relationships are referred to as ‘horizontal’, as they involve only European-level bodies.

Horizontal relationships in supra-national enforcement

The European-level layer of enforcement includes a variety of bodies, not only the European Commission but also sectoral networks and boards established under different legal frameworks. This plurality raises the question of how coordination among these supranational actors should be managed. When these bodies act under the same regulatory framework, their respective mandates are usually clearly

defined and complementary. However, from a cross-framework perspective, there are no established mechanisms to coordinate their activities, which becomes problematic when the same conduct falls under multiple overlapping legal regimes.

Horizontal relationships within a single framework

From an intra-framework perspective, the respective roles and responsibilities at the supranational level are often clearly defined. For instance, under the Digital Services Act, the European Board for Digital Services plays a primarily consultative role. It coordinates national enforcement actions in cases with a transnational dimension and provides support and advice to the European Commission, without exercising direct enforcement powers.

Conversely, there is no overarching framework ensuring comprehensive coordination among different European-level bodies, increasing the risk of horizontal conflicts from a cross-framework perspective.

Horizontal relationships from a cross-framework perspective

Sector-specific coordination bodies broadly lack institutionalised cooperation mechanisms, even though the European Commission, by its presence across many of them, may serve as *de facto* coordinating entity. Nonetheless, some regulations mention the possibility for EU-level bodies to cooperate. This is the case, for instance, for the European Artificial Intelligence Board, which includes the participation of the European Data Protection Supervisor, as well as any other body or authority whose expertise may be relevant on a case-by-case basis.⁸³² Similarly, the PAR explicitly mentions the possibility of cooperating with the European Board for Media Services,⁸³³ while the DSA foresees a dialogue between the European Board for Digital Services and the European Data Protection Board.⁸³⁴ These ‘soft’

⁸³² AI Act, Article 65(2) and 66(h).

⁸³³ PAR, Article 22(8).

⁸³⁴ DSA, Article 62 and Recital 134.

coordination mechanisms, though a welcome recognition of regulatory overlap, remain isolated and may prove insufficient to fully prevent conflicting decisions.

An example of horizontal overlap at the supranational level concerns the restriction of certain data combination practices, which, although governed by the GDPR, are now prohibited under the DMA.⁸³⁵ In this context, both the European Commission and national DPAs may seek to intervene on the same conduct. This is precisely the reason why the ‘pay-or-consent’ model adopted by Meta,⁸³⁶ which has been sanctioned by the European Commission for infringing the DMA,⁸³⁷ had first been the subject of an opinion issued by the EDPB assessing its compatibility with the GDPR.⁸³⁸ In such a scenario, not only there is a potential vertical conflict between the Commission and national DPAs, but also a possible horizontal conflict at the supranational level between the Commission and the EDPB. This stems from the fact that, while the Commission may take the EDPB’s opinion into account when assessing the same practice under the DMA, it is not legally bound to do so. At this stage, it remains unclear whether the EDPB’s position influenced the Commission’s decision, as the full text of its decisions has not been published. This case thus illustrates the potential for parallel, and possibly diverging, legal assessments of the same practice, raising questions about consistency of positions taken by EU-level bodies.

The types of overlaps at the supranational level presented in this section can lead to various horizontal conflicts in the enforcement of the EU digital acquis, as summarised in Table 7.

Table 7. Types of horizontal overlaps at the supranational level

⁸³⁵ See *supra*: Chapter IV, Section 2.

⁸³⁶ See *supra*: Chapter IV, Section 2..

⁸³⁷ European Commission, ‘Commission finds Apple and Meta in breach of the Digital Markets Act’ (n 646).

⁸³⁸ European Data Protection Board, ‘Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms’ (n 645).

<i>Horizontal Relationships</i>	
<i>Intra-framework Overlaps</i>	EU authorities competent under the same legal regime
<i>Example</i>	EU Commission vs European Board for Digital Services
<i>Cross-framework Overlaps</i>	EU authorities competent under different legal regimes
<i>Example</i>	EU Commission vs EDPB

Given these complexities, ensuring effective enforcement requires acknowledging the substantial overlaps in regulations affecting digital platforms and designing mechanisms to mitigate conflicts and enhance coordination among authorities at different levels.

CONCLUDING REMARKS

The EU's effort to regulate digital platforms reflects a strong political commitment to shaping the digital space in accordance with European values. Yet, the growing density of regulatory instruments, from the GDPR to the AI Act, has given rise to a fragmented and overlapping landscape that challenges effective enforcement. As digital services often operate interdependently, a single actor may simultaneously fall under multiple classifications, including digital platform, data processor, and AI deployer, and thus be subject to several regulatory regimes at once.

These overlaps are reflected in the growing number of national and supranational authorities that may assert competence over the same case. A key distinction has been drawn between intra-framework coordination, which concerns situations where multiple authorities are competent under the same legal instrument, and cross-framework coordination, which arises when different regulatory regimes apply concurrently. While the former is generally supported by formal cooperation mechanisms that help manage cross-border cases and allocate competences

between different authorities, the latter remains largely unaddressed. The result is a multiplication of competent authorities even within a single Member State, compounded by additional complexities in cross-border cases and the partial centralisation of enforcement under certain regulation. This patchwork of enforcement structures risks undermining the effectiveness of the EU's digital agenda, particularly when dealing with major actors, such as VLOPs and Gatekeepers.

To address this complexity, the EU should consider moving toward more integrated enforcement structures. While substantive overlaps are currently under scrutiny within the Digital Omnibus Strategy, special attention should be paid to designing an enforcement architecture capable of applying the relevant regulations in a consistent and coordinated manner, thereby ensuring a holistic approach of digital harms. At least three main solutions can be considered and possibly combined to address the questionable framework of public enforcement in European digital policy, ranging from more achievable to more ambitious.⁸³⁹ A first solution could consist in enhancing coordination tools following the model of the recently adopted guidelines on the interplay among different frameworks, potentially coupled with the establishment of dedicated forums for consultation or digital clearinghouses.⁸⁴⁰ A second solution could consist in the establishment, through the adoption of a horizontal framework, of binding conflict-resolution mechanisms in cases of overlaps. A third solution comprises the centralisation of enforcement powers at the EU level for major platforms, potentially using the notion of 'VLOPs' as a common reference point across frameworks. Such centralisation could imply an extension of

⁸³⁹ These solutions are further analysed in a forthcoming paper: Giovanni De Gregorio and Anna Vicinanza, 'Enforcing the EU Digital Acquis: Overlaps and Possible Pathways' (Yearbook of European Law, Forthcoming, 2026).

⁸⁴⁰ European Data Protection Supervisor, 'Towards a Digital Clearinghouse 2.0' (2025) <<https://www.edps.europa.eu/data-protection/our-work/publications/other-documents/2025-01-15-towards-digital-clearinghouse-20>> accessed 28 January 2025.

the European Commission's current enforcement competences, but the creation of an independent European agency could also be foreseen.⁸⁴¹

While more far-reaching reforms may offer greater systemic effectiveness, they face significant obstacles, both in terms of building political consensus and ensuring compliance with the limits set by EU primary law. In this perspective, advancing the more achievable solutions would already mark meaningful progress. Choosing inaction, on the other hand, carries the real risk of replicating, or even exacerbating, the enforcement shortcomings observed under previous frameworks, most notably the GDPR. Although enforcement design has not traditionally been central to EU regulatory efforts, largely due to the principle of national procedural autonomy, the scale and ambition of today's digital legislation demand enforcement mechanisms capable of matching their scope. The capacity of the EU to scrutinise the way platforms intervene on content transmission strongly depends on effective coordination and a holistic understanding of digital regulation.

⁸⁴¹ Bastos and Pałka (n 720).

CONCLUSIONS

The World Wide Web decreased the cost for content production and distribution, widening the opportunities for individual and collective expression. However, the information-abundant environment of the Internet paved the way for the success of digital services consisting in content organisation. In this context, information distribution channels have become increasingly concentrated in the hands of a few large platforms, which have emerged as crucial intermediaries in today's public sphere.⁸⁴² By intermediating a significant share of global interactions, platforms can unilaterally determine the dynamics of information flows. This gatekeeping role concerns not only commercial exchanges but also *latu sensu* political information, conferring upon platforms an opinion power comparable to that of traditional media industries such as broadcasters.

Similarly to legacy media actors, platforms possess the power to select which content reaches the audience, thereby shaping the formation of public opinion. Content selection is performed through extensive filtering activities that determine which third-party information is excluded or prioritised. The capacity to block the transmission of certain information relates to content moderation, while all transmitted content is also ranked, prioritised and recommended to users.

Opinion power is inherently linked to political power because of the role of public opinion in legitimising governments and political action. Consequently, democracies have traditionally regulated opinion power to promote the public interest in a plural, rich, unbiased and transparent public debate. A similar goal of aligning the digital environment closer to the public interest and democratic values has been indirectly pursued at the European Union level through the adoption of certain pioneering regulatory frameworks.⁸⁴³ These include the GDPR, adopted in

⁸⁴² Bradford (n 2) 6.

⁸⁴³ Bradford (n 2) 10.

2016 to foster the protection of the fundamental right to privacy online, the Digital Services Package, the Media Freedom Act, the Regulation on Transparency and Targeting of Political Advertising, and the AI Act.

This research had the purpose to assess the role of these frameworks in limiting digital platforms' unilateral control on information flows. Overall, the emerging picture is nuanced: undeniable progress has been achieved in some areas, yet several issues remain unclear or insufficiently addressed.

On a preliminary note, it should be noted that platforms' power to curate content, through both moderation and prioritisation practices, has been preserved. An obligation to act as neutral carriers, prohibited from intervening on content transmission, has not been embraced. Rather, the new regulations can be framed as an effort to *counterbalance* platforms' unilateral filtering power and to promote an increased democratisation of the online public sphere.⁸⁴⁴ Several provisions significantly enhance platforms' *accountability* for their content curation choices,⁸⁴⁵ subjecting their activities to external scrutiny and providing prerogatives to diverse stakeholders.

The new rules present a substantial development of the traditional *safe harbour* framework, under which platforms benefited from a right to intervene on content transmission without corresponding responsibilities. At that time, content management was entirely entrusted to these actors, without any public interest consideration involved: except where national law allowed injunctions, platforms were free to ignore illegal content while removing legal content. One major advancement of the DSA concerns precisely greater external oversight on illegal content online. Public authorities, users, and civil society organisations certified as trusted flaggers now possess the right to have their reports on illegal content

⁸⁴⁴ De Gregorio, *Digital Constitutionalism in Europe*, 3.

⁸⁴⁵ Husovec, *Principles of the Digital Services Act* (n 339).

examined by platforms, whose inaction may trigger liability. Moreover, major platforms designated as VLOPs or VLOSEs are required to mitigate the risk of disseminating illegal and harmful content through their services. It remains unclear, however, whether such obligations require a degree of proactive content monitoring or merely the adaptation of service design to avoid facilitating the spread of harmful material (for instance, by limiting virality mechanisms). In any case, the adequacy of these mitigation measures is subject to centralised oversight by the European Commission, which thus becomes another key actor in supervising the diffusion of illegal content online.

With regard to spontaneous moderation practices, platforms retain the power to block information transmission but are now subject to a series of obligations. First, when performing voluntary monitoring on content transmission, they have a duty to report serious illegal activities eventually encountered and removed. Then, a major contribution of the DSA lies in the introduction of procedural safeguards, including the obligation to provide a statement of reasons for content restrictions and access to redress mechanisms, including out-of-court dispute settlement bodies. These safeguards represent a significant improvement for users' rights, reducing arbitrariness and facilitating external scrutiny. Notably, they also apply to demotion practices within recommender systems, known as *shadow-banning*, which had traditionally been conducted in a non-transparent manner. Moreover, some procedural safeguards are strengthened by the Media Freedom Act when the affected user qualifies as a media service, thereby recognising a privilege to the media in moderation processes.

In addition, platforms are now subject to a general obligation to respect fundamental rights when restricting content. While this provision endorses the idea of fundamental rights governance by private actors, it also constitutes a progress compared to the previous framework, where platforms already performed such role without oversight by public authorities or courts from a fundamental rights perspective. The obligation to respect fundamental rights may also affect the rule-

making power of platforms, as it could enable public authorities to deem certain grounds for removal excessively restrictive of free speech and therefore unlawful. The duty to respect fundamental rights in moderation processes is reiterated within the systemic risks management framework applicable to VLOPs and VLOSEs. Under this system, large platforms must justify their balancing of competing interests in moderation decisions, finding an *equilibrium* between laissez-faire approaches and excessive interventionism. However, the precise point of equilibrium remains uncertain, depending on each platform's internal assessment and the European Commission's subsequent evaluation. Further legal certainty may derive from the adoption of codes of conduct or guidelines.

Turning to content prioritisation and recommendation, i.e. the second major type of filtering performed by platforms, the counterbalancing effect appears more limited. These practices are explicitly addressed by the DSA, the DMA, and the Regulation on Political Advertisement. The AI Act, conversely, while being applicable to machine learning recommender systems, does not seem to add any specific requirement in this context, except for a broad prohibition of manipulation and exploitation of vulnerabilities.

In contrast to offline communication industries, digital platforms heavily rely on microtargeted prioritisation based on the collection of personal data. Because of the crucial role of personal data in this context, recent frameworks build upon and complement the GDPR through two main approaches. First, they reinforce the requirement for user consent to targeted recommendations by mandating that an *alternative but equivalent* option with reduced profiling practices is offered. Second, they prohibit particularly dangerous targeting practices, such as advertising based on profiling using sensitive data or directed at minors. In addition to these restrictions on targeting practices, recent regulations have introduced a series of explanatory duties related to recommender systems, as well as other transparency obligations, such as the public repository for advertisements.

These provisions appear to have been designed to prevent user manipulation, partly through limiting targeting practices, partly through enhanced algorithmic transparency. Nevertheless, the functioning of recommender systems remains largely determined unilaterally by platforms, with limited powers granted to users and other external actors. Users may choose to receive less personalised advertising,⁸⁴⁶ refuse targeted political advertising,⁸⁴⁷ and access an unfiltered version of major platform services.⁸⁴⁸ Yet, these options represent rigid binary choices rather than tools for active personalisation or calibration of recommendation parameters.⁸⁴⁹ From this perspective, content recommendation mechanisms appear less pluralistic than content moderation under the new frameworks. Furthermore, restrictive interpretation of the rules, such as in the case of the *pay-or-consent* model, may additionally reduce users' choices. However, the systemic risk management obligations applicable to VLOPs and VLOSEs also extend to recommender systems and can significantly alter the regulatory landscape. Indeed, these rules allow the European Commission to scrutinise whether algorithms are adequately designed to safeguard, for instance, user autonomy or their access to plural and relevant information.

The open-ended nature of provisions on risk assessment, combined with traditional structural weaknesses in enforcing rules on Big Tech, highlights the importance of the oversight architecture. Marking a departure from the EU's traditionally minimal enforcement rules, the Digital Services Package represents a decisive step forward, particularly by introducing a centralised model centred on the European Commission. However, the effective implementation of digital platforms regulation requires a holistic approach, encompassing the complementary application of the DSA, GDPR, DMA, EMFA, PAR, and AI Act. To achieve it, supervisory

⁸⁴⁶ DMA, Article 5(1).

⁸⁴⁷ PAR, Article 18.

⁸⁴⁸ DSA, Article 38.

⁸⁴⁹ Reviglio and Fabbri (n 571).

authorities operating under sectoral frameworks must coordinate within a harmonised procedural system, hopefully coupled with symmetrical centralisation when addressing major platforms. In this context, the establishment of an independent European supervisory agency should be considered to avoid interference – or even perception of interference – with other political priorities when the Commission acts as central enforcer.⁸⁵⁰

Overall, this research found clear progress in embedding the public interest within the governance of online information flows. However, several critical aspects remain. First, EU legislators have devoted greater attention to moderation practices than to content recommendation. While moderation is directly connected to free speech, the impact of recommender systems on public opinion is more of a structural nature and needs to be equally addressed. In this regard, a key step forward would be to enable users to increasingly control the inputs and parameters for content curation algorithms. Second, the systemic risks provisions applicable to VLOPs and VLOSEs operate as *blank rules*, whose vagueness complicates the assessment on the impact of the DSA on platforms' unilateral content curation power, as much depends on platforms' implementation and the Commissions' subsequent evaluation. Third, despite the DSA and the DMA's attention to enforcement, a significant asymmetry in enforcement structures is observable across regulatory frameworks. Cross-framework coordination rules between national and supranational authorities are urgently needed to achieve a complementary implementation of EU digital regulations.

Finally, a pressing challenge concerns the rise of new, potentially dominant information distributors in the online public sphere. The growing reliance on generative AI models for accessing information reopens the issue of regulatory intervention aimed at counterbalancing unilateral control over content selection.

⁸⁵⁰ Buri (n 349); Hert and Hajduk (n 712) 297.

Since these models generate their own outputs, they do not systematically fall within the category of intermediaries under the Digital Services Act, nor within the list of core platforms services under the Digital Markets Act. Conversely, the Regulation on Political Advertising will apply as soon as they begin offering advertising services, which, according to recent public statements by industry leaders, is occurring in the very near future. The AI Act, meanwhile, remains largely silent on content selection, although this aspect could arguably be addressed within its general provisions on systemic risk assessment. While the European Commission seems to be aware of this regulatory gap, the current deregulatory momentum, partly fuelled by geopolitical tensions, risks slowing further progress in this area. Yet the need to subject emerging dominant opinion intermediaries to a public-interest framework cannot be overlooked, as it is crucial for the functioning of our democratic societies.

BIBLIOGRAPHY

Albert J, 'Researcher Access to Platform Data: Experts Weigh in on the Delegated Act' (*DSA Observatory*, 29 November 2024) <<https://dsa-observatory.eu/2024/11/29/researcher-access-to-platform-data-experts-weigh-in-on-the-delegated-act/>> accessed 21 May 2025

——, 'DSA Risk Assessment Reports: A Guide to the First Rollout and What's next' (*DSA Observatory*, 9 December 2024) <<https://dsa-observatory.eu/2024/12/09/dsa-risk-assessment-reports-are-in-a-guide-to-the-first-rollout-and-whats-next/>> accessed 7 February 2025

——, 'TikTok and the Romanian Elections: A Stress Test for DSA Enforcement - DSA Observatory' (20 December 2024) <<https://dsa-observatory.eu/2024/12/20/tiktok-and-the-romanian-elections/>> accessed 8 September 2025

Allen A, 'New EU Rules on Political Advertising Set to Have Limited Impact on Advertising Ecosystem' (*Center for Democracy and Technology*, 20 March 2024) <<https://cdt.org/insights/new-eu-rules-on-political-advertising-set-to-have-limited-impact-on-advertising-ecosystem/>> accessed 20 February 2025

Allyn B, 'Online News Publishers Face "extinction-Level Event" from Google's AI-Powered Search' *NPR* (31 July 2025) <<https://www.npr.org/2025/07/31/nx-s1-5484118/google-ai-overview-online-publishers>> accessed 11 October 2025

Amnesty International, 'Myanmar: The Social Atrocity: Meta and the Right to Remedy for the Rohingya' (Amnesty International 2022) <<https://www.amnesty.org/en/documents/asa16/5933/2022/en/>> accessed 19 March 2025

Ananny M, 'From Noxious to Public? Tracing Ethical Dynamics of Social Media Platform Conversions' (2015) 1 *Social Media + Society* <<https://doi.org/10.1177/2056305115578140>> accessed 13 November 2024

António Guterres, 'Social Media Platforms Based on a Business Model That Monetizes Anger & Negativity Are Causing Untold Damage to Societies. Hate Speech & Misinformation Are Proliferating. Our Data Is Being Bought & Sold to Influence Behaviour. We Need Regulatory Frameworks to Change This.' <<https://x.com/antonioguterres/status/1574111500201074688>> accessed 29 October 2025

Appelman N, 'Research Report on Disparate Content Moderation' (*DSA Observatory*, 31 October 2023) <<https://dsa-observatory.eu/2023/10/31/research-report-on-disparate-content-moderation/>> accessed 6 March 2025

Aristotele, *Politica* (1993rd edn, Economica Laterza 4th century BCE)

Article 19, ‘The Implication of the Proposed EU Political Advertising Regulation for Freedom of Expression’ <https://www.article19.org/wp-content/uploads/2023/08/A19-The-implications-of-the-Proposed-EU-Political-Advertising-Regulation-A19_clean.pdf>

Autorità Garante delle Comunicazioni, ‘Delibera 325/23/CONS. Richiesta Di Parere Dell’Autorità Garante Della Concorrenza e Del Mercato in Merito al Procedimento Avviato Nei Confronti Di Tik Tok Italy S.r.l. in Materia Di Pratiche Commerciali Scorrette PS/12543’ <<https://www.agcom.it/provvedimenti/delibera-325-23-cons>>

——, ‘Delibera 110/24/CONS. Richiesta Di Parere Dell’Autorità Garante Della Concorrenza e Del Mercato in Merito al Procedimento Avviato Nei Confronti Di Meta Platforms Inc. e Meta Platforms Ireland Limited in Materia Di Pratiche Commerciali Scorrette PS/12566.’ <<https://www.agcom.it/provvedimenti/delibera-110-24-cons-0>>

Baker CE, *Media Concentration and Democracy: Why Ownership Matters* (Cambridge University Press 2006) <<https://www.cambridge.org/core/books/media-concentration-and-democracy/31C4D0D3746C15CA199EF62B9772B068>> accessed 13 November 2024

Baldwin R, Cave M and Lodge M, ‘Enforcing Regulation’ in Robert Baldwin, Martin Cave and Martin Lodge (eds), *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press 2011) <<https://doi.org/10.1093/acprof:osobl/9780199576081.003.0011>> accessed 13 January 2026

Balkin JM, ‘Moody v. NetChoice - The Supreme Court Meets the Free Speech Triangle’ [2025] Yale Law School, Public Law Research Paper <<https://papers.ssrn.com/abstract=5104013>> accessed 8 October 2025

Barata J, ‘Protecting Media Content on Social Media Platforms’ [2022] Verfassungsblog <<https://verfassungsblog.de/emfa-dsa/>> accessed 13 November 2024

Barlow JP, ‘A Declaration of the Independence of Cyberspace’ <<https://www.eff.org/cyberspace-independence>> accessed 21 October 2025

Barwise P and Watkins L, ‘The Evolution of Digital Dominance. How and Why We Got to GAFA’ in Damian Tambini and Martin Moore, *Digital Dominance. The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018)

Bastos FB and Pałka P, ‘Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?’ (2023) 19 *European Constitutional Law Review* 487 <<https://www.cambridge.org/core/journals/european-constitutional-law-review/article/is-centralised-general-data-protection-regulation-enforcement-a-constitutional-necessity/65F232075D5ED87A1CE1E8F642E82206>> accessed 13 February 2025

Becker S, ‘Political Negotiations Continue: EU Lawmakers Fail to Agree on Strong Rules for Regulating Political Advertising’ (*European Digital Rights (EDRi)*, 12 October 2023) <<https://edri.org/our-work/political-negotiations-continue-eu-lawmakers-fail-to-agree-on-strong-rules-for-regulating-political-advertising/>> accessed 21 February 2025

Becker S and Penfrat J, ‘The DSA Fails to Reign in the Most Harmful Digital Platform Businesses – But It Is Still Useful’ in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023)

Bell E, ‘Silicon Valley and Journalism: Make up or Break up? | Reuters Institute for the Study of Journalism’ <<https://reutersinstitute.politics.ox.ac.uk/news/silicon-valley-and-journalism-make-or-break>> accessed 21 October 2025

Benckert A, ‘We’re Updating Our Terms of Service to Better Explain How Facebook Works’ (*Meta*, 27 June 2019) <<https://about.fb.com/news/2019/06/updating-our-terms/>> accessed 19 February 2025

Bernard T, ‘Reading the Systemic Risk Assessments for Major Speech Platforms: Notes and Observations’ (*Tech Policy Press*, 20 December 2024) <<https://techpolicy.press/reading-the-systemic-risk-assessments-for-major-speech-platforms-notes-and-observations>> accessed 7 February 2025

Bertelli G and Raposio J, ‘ISP Liability: Are Platforms like YouTube Directly Liable for Illegal Uploads?’ (*MediaLaws*, 15 September 2020) <<https://www.medialaws.eu/isp-liability-are-platforms-like-youtube-directly-liable-for-illegal-uploads/>> accessed 14 May 2025

Bertolini A, Episcopo F and Cherciu N-A, ‘Liability of Online Platforms’ (European Parliamentary Research Service 2021) PE 656.318

Bertuzzi L, ‘Media Exemption Ruled out in DSA Negotiations, but Could Return’ (*Euractiv*, 24 November 2021) <<https://www.euractiv.com/section/digital-single-market/news/media-exception-ruled-out-in-dsa-negotiations-but-could-return/>> accessed 9 May 2025

Bianchi T, 'Online Search Market in Europe – Statistics & Facts' (*Statista*, 27 May 2024) <<https://www.statista.com/topics/11065/online-search-market-in-europe/>> accessed 7 January 2025

——, 'Global Top Websites by Monthly Visits 2024' <<https://www.statista.com/statistics/1201880/most-visited-websites-worldwide/>> accessed 24 June 2025

Blanc F and Faure MG, 'Smart Enforcement. Theory and Practice' (Social Science Research Network, 1 November 2018) <<https://papers.ssrn.com/abstract=3372956>> accessed 13 January 2026

Bogost I, 'The Age of Social Media Is Ending' (*The Atlantic*, 10 November 2022) <<https://www.theatlantic.com/technology/archive/2022/11/twitter-facebook-social-media-decline/672074/>> accessed 21 October 2025

Bogucki A and others, 'The AI Act and Emerging EU Digital Acquis' (CEPS 2022) <<https://www.ceps.eu/ceps-publications/the-ai-act-and-emerging-eu-digital-acquis/>> accessed 13 January 2026

Booth R and editor RBU technology, 'ChatGPT “Upgrade” Giving More Harmful Answers than Previously, Tests Find' *The Guardian* (14 October 2025) <<https://www.theguardian.com/technology/2025/oct/14/chatgpt-upgrade-giving-more-harmful-answers-than-previously-tests-find>> accessed 21 October 2025

Botero Arcila B, 'An Early Win for the Transparency Measures of the DSA. A Comment on Amazon Services v. European Commission (C-638/23)' (*DSA Observatory*, 2 May 2024) <<https://dsa-observatory.eu/2024/05/02/an-early-win-for-the-transparency-measures-of-the-dsa-a-comment-on-amazon-services-v-european-commission-c-638-23/>> accessed 3 February 2025

Bovermann M, 'Putting X's Community Notes to the Test' [2024] *Verfassungsblog* <<https://verfassungsblog.de/putting-xs-community-notes-to-the-test/>> accessed 23 September 2025

Bradford A, 'Digital Empires: The Global Battle to Regulate Technology' [2023] *Faculty Books* <<https://scholarship.law.columbia.edu/books/367>>

——, 'Europe's Digital Constitution' [2023] *Verfassungsblog* <<https://verfassungsblog.de/europes-digital-constitution/>> accessed 23 September 2025

Brogi E, 'The European Media Freedom Act: Media Freedom, Freedom of Expression and Pluralism' (Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, European

Parliament 2023) PE 747.930
<[https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2023\)747930](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)747930)> accessed 13 November 2024

Bucher T, 'Want to Be on the Top? Algorithmic Power and the Threat of Invisibility on Facebook' (2012) 14 *New Media & Society* 1164
<<https://doi.org/10.1177/1461444812440159>> accessed 21 November 2024

Buri I, 'A Regulator Caught Between Conflicting Policy Objectives. Reflections on the European Commission's Role as DSA Enforcer' in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023)

Carlyle T, *On Heroes, Hero-Wo and the Heroic in History* (1906th edn, Longmans 1841)

Casey N, 'The Campaign to Make It Illegal for ChatGPT to Criticize Trump' (*Platformer*, 15 July 2025) <<https://www.platformer.news/andrew-bailey-chatgpt-trump-jawboning-legal-case/>> accessed 15 September 2025

Castells M, 'Communication, Power and Counter-Power in the Network Society' (2007) 1 *International Journal of Communication* 29
<<https://ijoc.org/index.php/ijoc/article/view/46>> accessed 13 November 2024

Cauffman C and Goanta C, 'A New Order: The Digital Services Act and Consumer Protection' (2021) 12 *European Journal of Risk Regulation* 758
<<https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/new-order-the-digital-services-act-and-consumer-protection/8E34BA8A209C61C42A1E7ADB6BB904B1>> accessed 13 November 2024

Chapman P, 'Advancing Platform Accountability: The Promise and Perils of DSA Risk Assessments' (*Tech Policy Press*, 9 January 2025)
<<https://techpolicy.press/advancing-platform-accountability-the-promise-and-perils-of-dsa-risk-assessments>> accessed 31 January 2025

Chee FY, 'TikTok Challenges EU Supervisory Fee, Following Meta's Footsteps' *Reuters* (8 February 2024) <<https://www.reuters.com/technology/tiktok-challenges-eu-supervisory-fee-following-metas-footsteps-2024-02-08/>> accessed 4 March 2025

——, 'Exclusive: Google's AI Overviews Hit by EU Antitrust Complaint from Independent Publishers' *Reuters* (4 July 2025)
<<https://www.reuters.com/legal/litigation/googles-ai-overviews-hit-by-eu-antitrust-complaint-independent-publishers-2025-07-04/>> accessed 11 September 2025

Cohen JE, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019)

Cohen N, 'Professor Makes the Case That Google Is a Publisher' *The New York Times* (21 May 2012) <<https://www.nytimes.com/2012/05/21/business/media/eugene-volokh-ucla-professor-makes-a-case-for-google-as-publisher.html>> accessed 19 March 2025

Committee of Ministers Council of Europe, 'Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the Roles and Responsibilities of Internet Intermediaries, Adopted by the Committee of Ministers on 7 March 2018 at the 1309th Meeting of the Ministers' Deputies' <<https://rm.coe.int/1680790e14>>

CompaniesMarketCap, 'Companies Ranked by Market Cap' (*CompaniesMarketCap.com*) <<https://companiesmarketcap.com/>> accessed 15 September 2025

Conger K and Hirsch L, 'Elon Musk Completes \$44 Billion Deal to Own Twitter' *The New York Times* (28 October 2022) <<https://www.nytimes.com/2022/10/27/technology/elon-musk-twitter-deal-complete.html>> accessed 25 March 2025

Corporate Europe Observatory, 'How Corporate Lobbying Undermined the EU's Push to Ban Surveillance Ads' (*Corporate Europe Observatory*, 18 January 2022) <<https://corporateeurope.org/en/2022/01/how-corporate-lobbying-undermined-eus-push-ban-surveillance-ads>> accessed 21 February 2025

Council of Europe, 'Council Conclusions on Support for Influencers as Online Content Creators' <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024XG03807>>

D'Amico A and others, 'Meta's Pay-or-Okay Model: An Analysis under EU Data Protection, Consumer and Competition Law' (2024) 2024 *Technology and Regulation* 254 <<https://techreg.org/article/view/19031>> accessed 7 February 2025

De Gregorio G, 'Il Diritto Delle Piattaforme Digitali: Un'analisi Comparata Dell'approccio Statunitense Ed Europeo al Governo Della Libertà Di Espressione' (2021) 50 *DPCE* Online <<https://www.dpceonline.it/index.php/dpceonline/article/view/1531>> accessed 9 October 2025

——, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022) <<https://www.cambridge.org/core/books/digital-constitutionalism-in-europe/A3F61C6368D17D953457234B8A59C502>> accessed 13 November 2024

De Gregorio G and Demkova S, 'The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe' *European Yearbook of Constitutional Law* 2024 (2024) <https://link.springer.com/chapter/10.1007/978-94-6265-647-5_10> accessed 20 May 2025

——, *Enforcing the EU Digital Acquis* (Digicon 2025)

——, 'Reordering the Enforcement of European Digital Regulation in Times on Omnibus' *Enforcing the EU Digital Acquis* (Digicon 2025)

De Gregorio G and Pollicino O, 'Auditing Platforms under the Digital Services Act' [2024] *Verfassungsblog* <<https://verfassungsblog.de/dsa-auditors-content-moderation-platform-regulation/>> accessed 21 May 2025

De Gregorio G and Vicinanza A, 'Enforcing the EU Digital Acquis: Overlaps and Possible Pathways' (Yearbook of European Law, Forthcoming, 2026)

Diakopoulos N and others, 'I Vote For - How Search Informs Our Choice of Candidate' in Damian Tambini and Martin Moore, *Digital Dominance. The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018)

Diaz A, 'Through the Google Goggles: Sociopolitical Bias in Search Engine Design' (2008)

Dijk (van) J, 'Social Media and the Culture of Connectivity' (*OUPblog*, 25 February 2013) <<https://blog.oup.com/2013/02/social-media-culture-connectivity/>> accessed 13 February 2026

Draghi M, 'The Future of European Competitiveness' (European Commission 2024) <https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en>

Eadicicco L, 'The next Era of Social Media Is Coming. And It's Messy so Far' *CNN* (11 October 2025) <<https://www.cnn.com/2025/10/11/tech/openai-sora-2-meta-ai-slop-social-media>> accessed 21 October 2025

——, 'The Battle for the Future of the Internet Is Underway | CNN Business' (*CNN*, 22 October 2025) <<https://www.cnn.com/2025/10/22/tech/openai-chatgpt-atlas-browser-google-chrome-ai>> accessed 27 October 2025

Edwards L and Veale M, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (Social Science Research Network, 23 May 2017) <<https://papers.ssrn.com/abstract=2972855>> accessed 13 November 2024

Elon Musk [@elonmusk], ‘Starlink Has Been Told by Some Governments (Not Ukraine) to Block Russian News Sources. We Will Not Do so Unless at Gunpoint. Sorry to Be a Free Speech Absolutist.’ <<https://x.com/elonmusk/status/1499976967105433600>> accessed 22 October 2025

Engel A, ‘Licence to Regulate: Article 114 TFEU as Choice of Legal Basis in the Digital Single Market’ in Annegret Engel, Xavier Groussot and Gunnar Thor Petursson (eds), *New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights* (Springer Nature Switzerland 2025) <https://doi.org/10.1007/978-3-031-65381-0_2> accessed 11 April 2025

‘Enrico Letta’s Report on the Future of the Single Market - Internal Market, Industry, Entrepreneurship and SMEs’ <https://single-market-economy.ec.europa.eu/news/enrico-lettas-report-future-single-market-2024-04-10_en> accessed 23 October 2025

Etteldorf C, ‘Why the Words “But” and “However” Determine the EMFA’s Legal Basis’ [2023] Verfassungsblog <<https://verfassungsblog.de/why-the-words-but-and-however-determine-the-emfas-legal-basis/>> accessed 11 April 2025

Euractiv, ‘EXCLUSIVE: US Limits Free Speech More than the EU, Says Tech Commissioner’ (*Euractiv*, 28 May 2025) <<https://www.euractiv.com/news/exclusive-us-limits-free-speech-more-than-the-eu-says-tech-commissioner/>> accessed 22 October 2025

——, ‘The Language of EUconomics’ (*Euractiv*, 4 October 2025) <<https://www.euractiv.com/news/the-secrets-of-eurospeak/>> accessed 22 October 2025

——, ‘Commission Checking If ChatGPT Falls under EU Online Governance Rules’ (*Euractiv*, 22 October 2025) <<https://www.euractiv.com/news/commission-checking-if-chatgpt-falls-under-eu-online-governance-rules/>> accessed 27 October 2025

Eurobarometer, ‘Media & News Survey 2023’ (European Parliament 2023) Flash Survey <<https://europa.eu/eurobarometer/surveys/detail/3153>>

Euronews and AP, ‘Donald Trump’s Twitter Ban Is “problematic,” Says Angela Merkel’ (*Euronews*, 12 January 2021) <<https://www.euronews.com/my-europe/2021/01/12/donald-trump-s-twitter-ban-is-problematic-says-angela-merkel>> accessed 24 March 2025

European Center for Digital Rights, ‘GDPR: A Culture of Non-Compliance?’ (noyb 2024) <https://noyb.eu/sites/default/files/2024-01/GDPR_a%20culture%20of%20non-compliance.pdf>

European Commission, ‘Communication 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/2017/0555 Final’ <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017DC0555>> accessed 7 October 2025

——, ‘Commission Staff Working Document | Impact Assessment Accompanying the Document | 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 | SWD/2020/348 Final’ <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020SC0348>> accessed 7 October 2025

——, ‘Communication from the Commission to the European Parliament, the Council, the European Social and Economic Committee and the Committee of the Regions on the European Democracy Action Plan’

——, ‘Speech by the President on inauguration of new US President’ (*European Commission*, 20 January 2021) <https://ec.europa.eu/commission/presscorner/detail/en/speech_21_167> accessed 25 March 2025

——, ‘Protecting Democracy’ (*European Commission*, 25 November 2021) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy_en> accessed 23 October 2025

——, ‘Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment’ <https://ec.europa.eu/commission/presscorner/detail/en/https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545> accessed 4 March 2025

——, ‘The EU’s Digital Services Act’ (*European Commission*, 27 October 2022) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en> accessed 21 October 2025

——, ‘The EU’s Digital Services Act’ (*European Commission*, 27 October 2022) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en> accessed 7 October 2025

——, ‘Antitrust: Commission Accepts Commitments by Amazon’ (*European Commission*, 20 December 2022)

<https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777> accessed 22 October 2025

——, ‘Digital Markets Act: Commission designates six gatekeepers’ <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328> accessed 18 February 2025

——, ‘Commission Sends Request for Information to Meta under the Digital Services Act’ (*Shaping Europe’s digital future* | *European Commission*, 19 October 2023) <<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-0>> accessed 24 March 2025

——, ‘Commission Sends Request for Information to TikTok under the Digital Services Act’ (*Shaping Europe’s digital future* | *European Commission*, 19 October 2023) <<https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-tiktok-under-digital-services-act>> accessed 24 March 2025

——, ‘Commission opens formal proceedings against X under the DSA’ (*European Commission*, 18 December 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709> accessed 25 March 2025

——, ‘Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act’ <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689> accessed 18 February 2025

——, ‘Commission Opens Formal Proceedings against TikTok under DSA’ (*European Commission*, 22 April 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487> accessed 8 September 2025

——, ‘Commission Opens Proceedings against TikTok under the DSA’ (*European Commission*, 22 April 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2227> accessed 13 October 2025

——, ‘Commission sends preliminary findings to Meta over its “Pay or Consent” model for breach of the Digital Markets Act’ <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3582> accessed 7 February 2025

——, ‘Commission Sends Requests for Information to YouTube, Snapchat, and TikTok on Recommender Systems under the Digital Services Act’ <<https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-youtube->

snapchat-and-tiktok-recommender-systems-under-digital> accessed 7 February 2025

——, ‘Commission and national authorities urge Temu to respect EU consumer protection laws’ (*European Commission*, 8 November 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5707> accessed 16 April 2025

——, ‘Commission fines Meta’ (*European Commission*, 14 November 2024) <https://ec.europa.eu/commission/presscorner/detail/sl/ip_24_5801> accessed 22 October 2025

——, ‘The Code of Conduct on Countering Illegal Hate Speech Online +’ (*Shaping Europe’s digital future* | *European Commission*, 20 January 2025) <<https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online>> accessed 21 March 2025

——, ‘The Code of Conduct on Disinformation’ (*Shaping Europe’s digital future* | *European Commission*, 13 February 2025) <<https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation>> accessed 21 March 2025

——, ‘Commission finds Apple and Meta in breach of the Digital Markets Act’ (*European Commission*, 23 April 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085> accessed 29 April 2025

——, ‘Delegated Act on Data Access under the Digital Services Act (DSA) | Shaping Europe’s Digital Future’ (*European Commission* | *Digital Strategy*, 2 July 2025) <<https://digital-strategy.ec.europa.eu/en/library/delegated-act-data-access-under-digital-services-act-dsa>> accessed 15 October 2025

——, ‘Commission Fines Google €2.95 Billion over Abusive Practices in Online Advertising Technology’ (*European Commission*, 5 September 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1992> accessed 22 October 2025

——, ‘DSA - Commission Preliminarily Finds TikTok and Meta in Breach of Their Transparency Obligations’ (*European Commission*, 24 September 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2503> accessed 26 October 2025

——, ‘Public Consultation on Joint Guidelines on the Interplay between DMA and GDPR’ (*European Commission* | *Digital Markets Act*, 9 October 2025)

<https://digital-markets-act.ec.europa.eu/public-consultation-joint-guidelines-interplay-between-dma-and-gdpr-2025-10-09_en> accessed 11 October 2025

——, ‘Commission Designates WhatsApp as Very Large Online Platform under the Digital Services Act |’ <<https://digital-strategy.ec.europa.eu/en/news/commission-designates-whatsapp-very-large-online-platform-under-digital-services-act>> accessed 11 February 2026

——, ‘Commission Investigates Grok and X’s Recommender Systems under the Digital Services Act’ <https://ec.europa.eu/commission/presscorner/detail/en/ip_26_203> accessed 3 February 2026

——, ‘Commission Guidelines on the Implementation of the Declaration Functionality for Media Service Providers Pursuant to Article 18 (1) of Regulation (EU) 2024/1083 (European Media Freedom Act)’ <<https://ec.europa.eu/newsroom/dae/redirection/document/124304>>

——, ‘2022 Strengthened Code of Practice on Disinformation | Shaping Europe’s Digital Future’ (*European Commission*) <<https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>> accessed 7 October 2025

——, ‘Commission Requests Information from X on Decreasing Content Moderation Resources under the Digital Services Act’ (*Shaping Europe’s digital future | European Commission*) <<https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-x-decreasing-content-moderation-resources-under-digital-services>> accessed 24 March 2025

——, ‘DMA Designated Gatekeepers’ (*European Commission*) <https://digital-markets-act.ec.europa.eu/gatekeepers_en> accessed 13 October 2025

——, ‘DSA: Making the Online World Safer | Shaping Europe’s Digital Future’ (*European Commission | Digital Strategy*) <<https://digital-strategy.ec.europa.eu/en/policies/safer-online>> accessed 8 October 2025

——, ‘Signatories of the 2022 Strengthened Code of Practice on Disinformation | Shaping Europe’s Digital Future’ (*Digital Strategy | European Commission*) <<https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation>> accessed 8 October 2025

——, ‘Supervision of the Designated Very Large Online Platforms and Search Engines under DSA’ (*Shaping Europe’s digital future | European Commission*) <<https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>> accessed 21 March 2025

——, ‘The Draghi Report on EU Competitiveness’ (*European Commission*) <https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en> accessed 23 October 2025

——, ‘The EU Code of Conduct on Countering Illegal Hate Speech Online’ <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en> accessed 7 October 2025

European Data Protection Board, ‘Interplay between the DSA and the GDPR: EDPB Adopts Guidelines’ (*European Data Protection Board*, 12 September 2025) <https://www.edpb.europa.eu/news/news/2025/interplay-between-dsa-and-gdpr-edpb-adopts-guidelines_en> accessed 15 September 2025

——, ‘Statement on the Digital Services Package and Data Strategy’ <https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-digital-services-package-and-data-strategy_en> accessed 20 January 2025

——, ‘Binding Decision 3/2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and Its Facebook Service (Art. 65 GDPR)’

——, ‘Urgent Binding Decision 01/2023 Requested by the Norwegian SA for the Ordering of Final Measures Regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR)’ <https://www.edpb.europa.eu/our-work-tools/our-documents/urgent-binding-decision-board-art-66/urgent-binding-decision-012023_en> accessed 18 February 2025

——, ‘Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms’ <https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en> accessed 18 February 2025

European Data Protection Supervisor, ‘Towards a Digital Clearinghouse 2.0’ (2025) <<https://www.edps.europa.eu/data-protection/our-work/publications/other-documents/2025-01-15-towards-digital-clearinghouse-20>> accessed 28 January 2025

European Parliament, ‘New EU Rules Needed to Address Digital Addiction’ (12 December 2023) <<https://www.europarl.europa.eu/news/en/press-room/20231208IPR15767/new-eu-rules-needed-to-address-digital-addiction>> accessed 29 October 2025

European Union Agency for Fundamental Rights, ‘GDPR in Practice – Experiences of Data Protection Authorities’ <<https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities>> accessed 11 April 2025

‘Former EU Commissioner and Activists Barred from US in Attack on European Tech Regulators’ *The Guardian* (24 December 2025) <<https://www.theguardian.com/technology/2025/dec/24/us-state-department-visa-ban-former-eu-commissioner-europe>> accessed 5 February 2026

Fowler GA, ‘Perspective | Shadowbanning Is Real: Here’s How You End up Muted by Social Media’ *Washington Post* (27 December 2022) <<https://www.washingtonpost.com/technology/2022/12/27/shadowban/>> accessed 4 March 2025

Franceschi-Bicchierai L, ‘Facebook Doesn’t Know What It Does With Your Data, Or Where It Goes: Leaked Document’ *VICE* (26 April 2022) <<https://www.vice.com/en/article/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes/>> accessed 3 February 2025

Frosio G, ‘Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy’ (Social Science Research Network, 6 February 2017) <<https://papers.ssrn.com/abstract=2912272>> accessed 13 November 2024

Frosio G and Geiger C, ‘Taking Fundamental Rights Seriously in the Digital Services Act’s Platform Liability Regime’ (2021) 29 *European Law Journal* 31 <<https://papers.ssrn.com/abstract=3747756>> accessed 13 November 2024

Furman J, *Unlocking Digital Competition* (2019) <<https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel>> accessed 24 June 2025

Geese A, ‘Why the DSA Could Save Us From the Rise of Authoritarian Regimes’ in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023)

Gillespie T, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (2018)

Gillet F, ‘Twitter Pulls out of Voluntary EU Disinformation Code’ (27 May 2023) <<https://www.bbc.com/news/world-europe-65733969>> accessed 4 March 2025

Gleick J, *The Information: A History, a Theory, a Flood* (Knopf Doubleday Publishing Group 2011)

Goanta C and Ortolani P, ‘Unpacking Content Moderation: The Rise of Social Media Platforms as Online Civil Courts’ (Social Science Research Network, 22

November 2021) <<https://papers.ssrn.com/abstract=3969360>> accessed 15 September 2025

Google Search, 'Filter or Blur Explicit Results with SafeSearch' (*Google Search Help*) <<https://support.google.com/websearch/answer/510?hl=en&co=GENIE.Platform%3DAndroid>> accessed 28 March 2025

Gorwa R, 'What Is Platform Governance?' (2019) 22 *Information, Communication & Society* 854 <<https://doi.org/10.1080/1369118X.2019.1573914>> accessed 13 November 2024

Gorwa R, Binns R and Katzenbach C, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7 *Big Data & Society* <<https://doi.org/10.1177/2053951719897945>> accessed 9 May 2025

Guzik A and Weigl L, 'In Brussels We Trust? Preliminary Insights Into the Legal Challenges to the DMA and DSA' (*Tech Policy Press*, 5 November 2024) <<https://techpolicy.press/in-brussels-we-trust-preliminary-insights-into-the-legal-challenges-to-the-dma-and-dsa>> accessed 3 February 2025

Habermas J, *Nuovo mutamento della sfera pubblica e politica deliberativa* (Raffaello Cortina Editore 2023)

Haeck P, 'EU Social Media Law Isn't Censorship, Tech Chief Tells US Critic' (*POLITICO*, 10 March 2025) <<https://www.politico.eu/article/social-media-law-does-not-regulate-speech-eu-tech-chief-tells-us-lawmaker-henna-virkkunen/>> accessed 23 September 2025

Harris B, 'An Update on Building a Global Oversight Board' (*Meta Newsroom*, 12 December 2019) <<https://about.fb.com/news/2019/12/oversight-board-update/>> accessed 8 October 2025

Haucap J and Heimeshoff U, 'Google, Facebook, Amazon, eBay: Is the Internet Driving Competition or Market Monopolization?' (2014) 11 *International Economics and Economic Policy*

Helberger N, 'The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power' (2020) 8 *Digital Journalism* 842 <<https://doi.org/10.1080/21670811.2020.1773888>> accessed 13 November 2024

——, 'Dealing with Opinion Power in the Platform World: Why We Really Have to Rethink Media Concentration Law' (2023) 11 *Digital Journalism* 1542 <<https://doi.org/10.1080/21670811.2022.2161924>> accessed 13 November 2024

Helberger N, Kleinen-von Königslöw K and Noll R, 'Regulating the New Information Intermediaries as Gatekeepers of Information Diversity' (2015) 17 Info 50

Helberger N, van Drunen M and Fahy R, 'The Platform-Media Relationship in the European Media Freedom Act' [2023] Verfassungsblog <<https://verfassungsblog.de/emfa-platforms/>> accessed 13 November 2024

Hert P de and Hajduk P, 'EU Cross-Regime Enforcement, Redundancy and Interdependence. Addressing Overlap of Enforcement Structures in the Digital Sphere after Meta.' (2024) 2024 Technology and Regulation 291 <<https://techreg.org/article/view/19322>> accessed 28 January 2025

Hinck S, 'Big Tech Antitrust Scrutiny Across the Atlantic' [2025] Verfassungsblog <<https://verfassungsblog.de/big-tech-antitrust-scrutiny-across-the-atlantic-meta-ftc-tech/>> accessed 22 October 2025

Hoboken J van and others, *Hosting Intermediary Services and Illegal Content Online: An Analysis of the Scope of Article 14 ECD in Light of Developments in the Online Service Landscape : Final Report* (Directorate-General for Communications Networks, Content and Technology (European Commission), Publications Office of the European Union 2019) <<https://data.europa.eu/doi/10.2759/284542>> accessed 13 November 2024

Holznagel D, 'Art. 21 DSA Has Come to Life' [2024] Verfassungsblog <<https://verfassungsblog.de/art-21-dsa-fundamental-rights-certification/>> accessed 15 May 2025

Horwitz J and others, 'The Facebook Files' *Wall Street Journal* (1 October 2021) <<https://www.wsj.com/articles/the-facebook-files-11631713039>> accessed 4 March 2025

House Judiciary Committee, 'Europe's Threat to American Speech and Innovation' <<http://judiciary.house.gov/committee-activity/hearings/europes-threat-american-speech-and-innovation>> accessed 23 September 2025

Husovec M, 'Will the DSA Work? On Money and Effort' in Joris van Hoboken (ed), *Putting the Digital Services Act Into Practice* (Verfassungbooks 2023)

——, *Principles of the Digital Services Act* (Oxford Academic 2024) <<https://academic.oup.com/book/58088>> accessed 13 November 2024

——, 'The Digital Services Act's Red Line: What the Commission Can and Cannot Do about Disinformation' (2024) 16 Journal of Media Law 47 <<https://doi.org/10.1080/17577632.2024.2362483>> accessed 23 September 2025

Husovec M and et al., ‘Re: Hearing on “Europe’s Threat to American Speech and Innovation”’ (3 September 2025) <<https://husovec.eu/wp-content/uploads/2025/09/US-Academic-Letter-DSA-Censorship.pdf>>

Husovec, Martin, ‘DSA – Monthly Active Users – Second Disclosure’ <<https://husovec.eu/wp-content/uploads/2023/09/DSA-MAU-Second-Disclosure-Aug2023.pdf>>

Iaia V, ‘I Complessi Contorni Della Nozione Di Pubblicità Politica Alla Prova Delle Elezioni Europee 2024’ (*MediaLaws*, 19 June 2024) <<https://www.medialaws.eu/21061-2/>> accessed 24 February 2025

Il Post, ‘Elon Musk continua a bisticciare col suo chatbot’ *Il Post* (1 July 2025) <<https://www.ilpost.it/2025/07/01/grok-elon-musk/>> accessed 11 September 2025

Ings R, ‘Romanian Elections: TikTokers and an Election Scandal’ (*BBC*, 29 April 2025) <<https://www.bbc.com/articles/cqx41x3gn5zo>> accessed 8 September 2025

Instagram, ‘Updates to the Sensitive Content Control’ (*Instagram Blog*, 6 June 2022) <<https://about.instagram.com/blog/announcements/updates-to-the-sensitive-content-control>> accessed 25 February 2025

——, ‘Control Your Instagram Feed’ (*Instagram Blog*, 30 August 2022) <<https://about.instagram.com/blog/tips-and-tricks/control-your-instagram-feed>> accessed 25 February 2025

——, ‘Update on Political Content on Instagram and Threads’ (*Instagram*, 9 February 2024) <<https://about.instagram.com/blog/announcements/continuing-our-approach-to-political-content-on-instagram-and-threads>> accessed 25 February 2025

——, ‘New on Instagram: How to Reset Your Content Suggestions’ (*Instagram*, 19 November 2024) <<https://about.instagram.com/blog/announcements/reset-instagram-content-suggestions>> accessed 25 February 2025

Introna LD and Nissenbaum H, ‘Shaping the Web: Why the Politics of Search Engines Matters’ (2000) 16 *The Information Society* 169 <<https://doi.org/10.1080/01972240050133634>> accessed 26 June 2025

Jenkins H, *Convergence Culture: Where Old and New Media Collide* (NYU Press 2006) <<https://www.jstor.org/stable/j.ctt9qffwr>> accessed 18 September 2025

Kamara I and Bassini M, ‘The Cybersecurity and AI Nexus in the EU Digital Acquis’ [2025] *MediaLaws* <<https://www.medialaws.eu/rivista/the-cybersecurity-and-ai-nexus-in-the-eu-digital-acquis/>> accessed 13 January 2026

Keller D, ‘Comment to Council of Europe Committee of Ministers on the Draft Recommendation on Online Safety and Empowerment of Content Creators and Users’ (Social Science Research Network, 8 August 2025) <<https://papers.ssrn.com/abstract=5384268>> accessed 23 September 2025

Kemp S, ‘Digital 2025: Global Advertising Trends’ (*DataReportal – Global Digital Insights*, 5 February 2025) <<https://datareportal.com/reports/digital-2025-sub-section-global-advertising-trends>> accessed 24 June 2025

Kerkhof (van de) J, ‘Article 22 Digital Services Act: Building Trust with Trusted Flaggers’ (2025) 14 Internet Policy Review <<https://policyreview.info/articles/analysis/article-22-digital-services-act>> accessed 11 April 2025

Kern R, ‘Musk Changes Twitter Suspension Policy’ *Politico* (24 November 2022) <<https://www.politico.com/news/2022/11/24/musk-twitter-suspension-policy-00070819>> accessed 25 March 2025

——, ‘Twitter Stops Enforcing Covid-19 Misinformation Policy -’ *Politico* (29 November 2022) <<https://www.politico.com/news/2022/11/29/twitter-stops-enforcing-covid-19-misinformation-policy-00071110>> accessed 25 March 2025

Knutson R, ‘The Clash Between Facebook and Independent Researchers - WSJ Podcasts’ *Wall Street Journal* (9 August 2021) <<https://www.wsj.com/podcasts/the-journal/the-clash-between-facebook-and-independent-researchers/8fda97fc-203d-4632-bc86-f81c0cbe5faf>> accessed 23 May 2025

Kozak M, ‘Regulating Political Advertising’ [2023] *Verfassungsblog* <<https://verfassungsblog.de/regulating-political-advertising/>> accessed 10 February 2025

Kranjec J, ‘Google, Meta, and Amazon Generate Over 60% of Global Digital Advertising Revenue’ (*Stocklytics*, 29 February 2024) <<https://stocklytics.com/content/google-meta-and-amazon-generate-over-60-of-global-digital-advertising-revenue/>> accessed 24 June 2025

Kuczerawy A, ‘Remedying Overremoval’ in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023)

Lasorella G, ‘Relazione annuale 2025 sull’attività svolta e sui programmi di lavoro’ <https://www.agcom.it/sites/default/files/documenti/relazione_annuale/RELAZIONE%20ANNUALE%202025_0.pdf>

Le Monde, 'Le soutien problématique d'Elon Musk à Donald Trump' (22 October 2024) <https://www.lemonde.fr/idees/article/2024/10/22/le-soutien-problematique-d-elon-musk-a-donald-trump_6358082_3232.html> accessed 18 September 2025

Leerssen P, 'The DSA's First Shadow Banning Case' (*DSA Observatory*, 6 August 2024) <<https://dsa-observatory.eu/2024/08/06/the-dsas-first-shadow-banning-case/>, <https://dsa-observatory.eu/2024/08/06/the-dsas-first-shadow-banning-case/>> accessed 22 January 2025

——, 'From Murdoch to Musk: Platform Ownership and the Political Economy of Online Content Governance' (2025) 2 *Platforms & Society* 29768624251386260 <<https://doi.org/10.1177/29768624251386260>> accessed 26 October 2025

Leswing K and Subin S, 'Nvidia Briefly Touched \$4 Trillion Market Cap for First Time' (*CNBC*, 9 July 2025) <<https://www.cnbc.com/2025/07/09/nvidia-4-trillion.html>> accessed 15 September 2025

Letta E, 'Much More than a Market. Speed, Security, and Solidarity. Empowering the Single Market to Deliver a Sustainable Future and Prosperity for All EU Citizens' (2024) <<https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf>>

Lieb A and Chapekis A, 'Google Users Are Less Likely to Click on Links When an AI Summary Appears in the Results' (*Pew Research Center*, 22 July 2025) <<https://www.pewresearch.org/short-reads/2025/07/22/google-users-are-less-likely-to-click-on-links-when-an-ai-summary-appears-in-the-results/>> accessed 11 September 2025

'Lutnick Says EU Must Change Digital Rules for Steel Tariff Deal' *Bloomberg.com* (24 November 2025) <<https://www.bloomberg.com/news/articles/2025-11-24/lutnick-says-eu-must-change-digital-rules-for-steel-tariff-deal>> accessed 5 February 2026

MacKinnon R and others, 'Fostering Freedom Online: The Role of Internet Intermediaries'

Maelen CV and Griffin R, 'Twitter's Retreat from the Code of Practice on Disinformation Raises a Crucial Question: Are DSA Codes of Conduct Really Voluntary?' (*DSA Observatory*, 12 June 2023) <<https://dsa-observatory.eu/2023/06/12/twitters-retreat-from-the-code-of-practice-on-disinformation-raises-a-crucial-question-are-dsa-codes-of-conduct-really-voluntary/>> accessed 6 March 2025

Manzini P, 'Il Digital Market Act Decodificato' *Unione europea 2020 - I dodici mesi che hanno segnato l'integrazione europea* (Cedam Kluwer 2021)

——, 'Antitrust e Privacy: La Strana Coppia' in Pietro Manzini (ed), *I confini dell'antitrust. Diseguaglianze sociali, diritti individuali, concorrenza* (Giappichelli 2023)

Maroni M and Brogi E, 'Freedom of Expression and the Rule of Law: The Debate in the Context of Online Platform Regulation' in Pier Luigi Parcu and Elda Brogi (eds), *Research Handbook on EU Media Law and Policy* (Edward Elgar Publishing 2022)

Mastroianni R and Ferrario F, *Libertà di informazione e diritto dell'Unione europea. Le nuove sfide a tutela della democrazia e del pluralismo*. (Editoriale Scientifica 2022) <<https://www.libreriauniversitaria.it/liberta-informazione-diritto-unione-europea/libro/9791259764492>> accessed 13 November 2024

McSherry C and York JC, 'Content Moderation Is Broken. Let Us Count the Ways.' (*Electronic Frontier Foundation*, 29 April 2019) <<https://www.eff.org/deeplinks/2019/04/content-moderation-broken-let-us-count-ways>> accessed 8 April 2025

Merrill JB and Harwell D, 'Elon Musk's X Is Throttling Traffic to Websites He Dislikes' *The Washington Post* (15 August 2023) <<https://www.washingtonpost.com/technology/2023/08/15/twitter-x-links-delayed/>> accessed 25 March 2025

Meta, 'Facebook and Instagram to Offer Subscription for No Ads in Europe' (*Meta*, 12 November 2024) <<https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>> accessed 13 February 2025

——, 'Community Standards' (*Meta | Transparency Centre*) <<https://transparency.meta.com/policies/community-standards/>> accessed 26 October 2025

Miller M, 'New User Trends on Wikipedia' (*Diff*, 17 October 2025) <<https://diff.wikimedia.org/2025/10/17/new-user-trends-on-wikipedia/>> accessed 22 October 2025

Monti M, 'Why Online Public Discourse Needs a Media Privilege: In Defence of Article 18 of the EMFA' (*Centre for Media Pluralism and Media Freedom | EMFA Observatory*, 1 November 2024) <<https://cmpf.eui.eu/in-defence-of-article-18-of-the-emfa/>> accessed 11 February 2026

Moore M, *Tech Giants and Civic Power* (CMCP, Policy Institute, King's College London 2016)

Mosseri A, 'Control Your Instagram Feed with Favorites and Following' (*Instagram Blog*) <<https://about.instagram.com/blog/announcements/favorites-and-following>> accessed 7 February 2025

Moynihan Q and Asenjo A, 'Facebook Quietly Ditched the "It's Free and Always Will Be" Slogan from Its Homepage' *Business Insider* (27 August 2019) <<https://www.businessinsider.com/facebook-changes-free-and-always-will-be-slogan-on-homepage-2019-8>> accessed 18 February 2025

Murray C, 'All The Major Companies And Orgs Dumping Their DEI Programs (Full List)' (*Forbes*) <<https://www.forbes.com/sites/conormurray/2025/04/11/ibm-reportedly-walks-back-diversity-policies-citing-inherent-tensions-here-are-all-the-companies-rolling-back-dei-programs/>> accessed 18 September 2025

Murthy D, 'Evaluating Platform Accountability: Terrorist Content on YouTube' (2021) 65 *American Behavioral Scientist* 800 <<https://doi.org/10.1177/0002764221989774>> accessed 7 January 2025

Napoli P, *Social Media and the Public Interest. Media Regulation in the Disinformation Age* (Columbia University Press 2019) <<https://cup.columbia.edu/book/social-media-and-the-public-interest/9780231184540>> accessed 13 November 2024

Napoli P and Caplan R, *When Media Companies Insist They're Not Media Companies and Why It Matters for Communications Policy* (2016)

Napoli PM, 'In Pursuit of Ignorance: The Institutional Assault on Disinformation and Hate Speech Research' (2025) 41 *The Information Society* 1 <<https://doi.org/10.1080/01972243.2024.2419105>> accessed 18 June 2025

Newman JM, 'Antitrust in Attention Markets: Definition, Power, Harm' (2020) Paper No. 3745839 University of Miami Legal Studies Research <Available at SSRN: <https://ssrn.com/abstract=3745839> or <http://dx.doi.org/10.2139/ssrn.3745839>>

Newman N, 'Digital News Report 2025' (Reuters Institute for the Study of Journalism 2025) <<https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025>> accessed 24 June 2025

Noyb, '28 NGOs Urge EU DPAs to Reject "Pay or Okay" on Meta' (*noyb*, 16 February 2024) <<https://noyb.eu/en/28-ngos-urge-eu-dpas-reject-pay-or-okay-meta>> accessed 18 February 2025

——, ‘Statement on EDPB “Pay or Okay” Opinion’ (*noyb*, 17 April 2024) <<https://noyb.eu/en/statement-edpb-pay-or-okay-opinion>> accessed 18 February 2025

Nunez M, ‘Former Facebook Workers: We Routinely Suppressed Conservative News’ (*Gizmodo*, 9 May 2016) <<https://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006>> accessed 25 March 2025

O’Donovan B, ““Unskippable” Ads to Feature on Facebook and Instagram’ *Raidió Teilifís Éireann (Rte)* (12 November 2024) <<https://www.rte.ie/news/2024/1112/1480520-facebook-ads/>> accessed 18 February 2025

OpenAI, ‘Test degli annunci in ChatGPT’ (*Open AI*, 9 February 2026) <<https://openai.com/it-IT/index/testing-ads-in-chatgpt/>> accessed 13 February 2026

Ortolani P, ‘If You Build It, They Will Come: The DSA “Procedure Before Substance” Approach’ in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023)

Ortutay B, ‘All about Section 230, a Rule That Made the Modern Internet’ (*AP News*, 28 May 2020) <<https://apnews.com/article/d3e09c4037e2fc17558492b9bdce1ecc>> accessed 13 March 2025

Papakonstantinou V and De Hert P, ‘The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of “Act-Ification”, “GDPR Mimesis” and “EU Law Brutality”’ (Social Science Research Network, 1 May 2022) <<https://papers.ssrn.com/abstract=4123313>> accessed 17 July 2025

Pariser E, *Il Filtro* (Il Saggiatore 2012) <<https://www.ilsaggiatore.com/libro/il-filtro>> accessed 13 November 2024

Pasquale F, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) <<https://www.jstor.org/stable/j.ctt13x0hch>> accessed 10 June 2025

——, ‘Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power’ (2016) No. 2016–24 University of Maryland Francis King Carey School of Law <<https://papers.ssrn.com/abstract=2779270>> accessed 13 November 2024

Paul K, ‘Instagram Users Accuse Platform of Censoring Posts Supporting Palestine’ *The Guardian* (18 October 2023)

<<https://www.theguardian.com/technology/2023/oct/18/instagram-palestine-posts-censorship-accusations>> accessed 7 January 2025

Penfrat J, ‘The EU’s Attempt to Regulate Big Tech: What It Brings and What Is Missing’ (*European Digital Rights (EDRI)*, 18 December 2020) <<https://edri.org/our-work/eu-attempt-to-regulate-big-tech/>> accessed 4 March 2025

Pennisi M, ‘Facebook, perché sulla homepage non c’è più scritto «è gratis»’ *Corriere della Sera* (28 August 2019) <https://www.corriere.it/tecnologia/19_agosto_28/facebook-perche-homepage-non-c-piu-scritto-gratis-sara-sempre-9498de42-c97a-11e9-89f2-27d7028d49f0.shtml> accessed 18 February 2025

Petit N, *Big Tech and the Digital Economy: The Moligopoly Scenario* (Oxford University Press 2020)

Petrescu P, ‘Google Organic Click-Through Rates in 2014’ (*Moz*, 1 October 2014) <<https://moz.com/blog/google-organic-click-through-rates-in-2014>> accessed 7 January 2025

Petrosyan A, ‘Internet and Social Media Users in the World 2025’ (*Statista*) <<https://www.statista.com/statistics/617136/digital-population-worldwide/>> accessed 30 July 2025

Pollicino O, ‘Rights-Proof Simplification: The DigCon Project’s Contribution to the EU’s Digital Omnibus Consultation’ (*MediaLaws*, 17 October 2025) <<https://www.medialaws.eu/rights-proof-simplification-the-digcon-projects-contribution-to-the-eus-digital-omnibus-consultation/>> accessed 22 October 2025

Primack D and Rosenberg S, ‘Tech Leaders Line up behind Trump’ (*Axios*, 16 July 2024) <<https://www.axios.com/2024/07/16/andreesen-horowitz-musk-trump>> accessed 18 September 2025

Quintais JP, Appelman N and Fahy R, ‘Using Terms and Conditions to Apply Fundamental Rights to Content Moderation’ (Social Science Research Network, 25 November 2022) <<https://papers.ssrn.com/abstract=4286147>> accessed 22 January 2025

Reddit, ‘Digital Services Act (DSA): Information for EU Users’ (*Reddit Help*, 15 August 2025) <<https://support.reddithelp.com/hc/en-us/articles/23595536875796-Digital-Services-Act-DSA-Information-for-EU-users>> accessed 27 October 2025

Reviglio U and Fabbri M, ‘The Regulation of Recommender Systems Under the DSA: A Transition from Default to Multiple and Dynamic Controls?’ (*DSA*

Observatory, 22 November 2024) <<https://dsa-observatory.eu/2024/11/22/the-regulation-of-recommender-systems-under-the-dsa-a-transition-from-default-to-multiple-and-dynamic-controls/>> accessed 13 December 2024

Robb L, Candy T and Deane F, 'Regulatory Overlap: A Systematic Quantitative Literature Review' [2022] *Regulation & Governance* - Wiley Online Library <<https://onlinelibrary.wiley.com/doi/10.1111/rego.12504>> accessed 5 June 2025

Roose K, 'In Pulling Trump's Megaphone, Twitter Shows Where Power Now Lies' *The New York Times* (9 January 2021) <<https://www.nytimes.com/2021/01/09/technology/trump-twitter-ban.html>> accessed 24 March 2025

Rosen J, 'The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google' (2012) 80 *Fordham Law Review* 1525 <<https://ir.lawnet.fordham.edu/flr/vol80/iss4/1>>

Rosenberg M, Confessore N and Cadwalladr C, 'How Trump Consultants Exploited the Facebook Data of Millions' *The New York Times* (17 March 2018) <<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>> accessed 24 February 2025

Ruscheimer H and others, 'Brave New World. Out-Of-Court Dispute Settlement Bodies and the Struggle to Adjudicate Platforms in Europe.' [2024] *Verfassungsblog* <<https://verfassungsblog.de/ods-dsa-user-rights-content-moderatin-out-of-court-dispute-settlement/>> accessed 10 April 2025

Sam Altman [@sama], 'We Made ChatGPT Pretty Restrictive to Make Sure We Were Being Careful with Mental Health Issues. We Realize This Made It Less Useful/Enjoyable to Many Users Who Had No Mental Health Problems, but given the Seriousness of the Issue We Wanted to Get This Right. Now That We Have' <<https://x.com/sama/status/1978129344598827128>> accessed 21 October 2025

Sartor G, 'The Secondary Liability of Online Intermediaries' in Pier Luigi Parcu and Elda Brogi (eds), *Research Handbook on EU Media Law and Policy* (Edward Elgar Publishing 2022)

Schepisi C (ed), 'Il Costituzionalismo Digitale Tra Stati Uniti e Europa' *Unione Europea, Pluralismo e Libertà dei Media dell'era digitale* (Editoriale Scientifica 2025)

Scholten M and Stähler L, 'Introduction to Research Handbook on the Enforcement of EU Law' *Research Handbook on the Enforcement of EU Law* (Edward Elgar Publishing 2023)

<<https://www.elgaronline.com/edcollchap/book/9781802208030/book-part-9781802208030-9.xml>> accessed 25 July 2025

Schwemer SF, 'Trusted Notifiers and the Privatization of Online Enforcement' (2019) 35 Computer Law & Security Review 105339 <<https://www.sciencedirect.com/science/article/pii/S0267364918304436>> accessed 9 May 2025

Scott M, '5 Things to Know about the Digital Services Act's First Risk Assessments and Audits' (*Tech Policy Press*, 11 December 2024) <<https://techpolicy.press/5-things-to-know-about-the-digital-services-acts-first-risk-assessments-and-audits>> accessed 21 May 2025

Seiling L, Klinger U and Ohme J, 'Non-Public Data Access for Researchers: Challenges in the Draft Delegated Act of the Digital Services Act' (*Tech Policy Press*, 5 December 2024) <<https://techpolicy.press/non-public-data-access-for-researchers-challenges-in-the-draft-delegated-act-of-the-digital-services-act>> accessed 21 May 2025

Shavell S, 'The Optimal Structure of Law Enforcement' in Robert Baldwin, Colin Scott and Christopher Hood (eds), *A Reader on Regulation* (Oxford University Press 1998) <<https://doi.org/10.1093/acprof:oso/9780198765295.003.0011>> accessed 13 January 2026

StatCounter, 'Social Media Stats Worldwide' <<https://gs.statcounter.com/social-media-stats/all/worldwide/2022>> accessed 24 June 2025

Statista Research Department, 'Largest Online Retailers in the U.S. 2023' <<https://www.statista.com/statistics/274255/market-share-of-the-leading-retailers-in-us-e-commerce/>> accessed 24 June 2025

Sterling T, 'EU Commission Looks to Cut Overlap in Tech Directives -Virkkunen' *Reuters* (27 March 2025) <<https://www.reuters.com/technology/eu-commission-looks-cut-overlap-tech-directives-virkkunen-2025-03-27/>> accessed 11 April 2025

Sunstein CR, *#Republic: Divided Democracy in the Age of Social Media* (NED-New edition, Princeton University Press 2018) <<https://www.jstor.org/stable/j.ctv8xnhtd>> accessed 13 November 2024

Suzor NP, *Lawless: The Secret Rules That Govern Our Digital Lives* (Cambridge University Press 2019) <<https://www.cambridge.org/core/books/lawless/8504E4EC8A74E539D701A04D3EE8D8DE>> accessed 13 November 2024

Tambini D, 'Social Media Power and Election Legitimacy' in Damian Tambini and Martin Moore, *Digital Dominance. The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018)

——, 'The EU Is Taking Practical Measures to Protect Media Freedom. Now We Need Theory.' (*Centre for Media Pluralism and Freedom*, 9 May 2023) <<https://cmpf.eui.eu/the-eu-is-taking-practical-measures-to-protect-media-freedom-now-we-need-theory/>> accessed 13 November 2024

Tambini D and Mazzoli EM, 'Prioritisation Undercovered. The Discoverability of Public Interest Content Online' (Committee of Experts on Media Environment and Reform, Council of Europe 2020) DGI(2020)19 <<https://www.coe.int/en/web/freedom-expression/-/discoverability-of-public-interest-content-online>> accessed 13 November 2024

The Economist, 'AI Is Killing the Web. Can Anything Save It?' *The Economist* (14 July 2025) <<https://www.economist.com/business/2025/07/14/ai-is-killing-the-web-can-anything-save-it>> accessed 15 September 2025

Thierer A, 'Celebrating 20 Years of Internet Free Speech & Free Exchange' (*Medium*, 21 June 2017) <<https://readplaintext.com/celebrating-20-years-of-internet-free-speech-free-exchange-8a10f236d0bd>> accessed 13 March 2025

Thierry Breton [@ThierryBreton], '#TikTok Has a Particular Obligation to Protect Children & Teenagers from Violent Content & Terrorist Propaganda —as Well as Death Challenges & Potentially Life-Threatening Content. #DSA Sets out Very Clear Obligations TikTok Must Comply with. Letter to TikTok CEO Shou Zi Chew' <https://t.co/J1tpVzXaYR> <<https://x.com/ThierryBreton/status/1712472108222329056>> accessed 27 October 2025

Thompson J, 'The New Visibility' (2005) 22 *Theory, Culture & Society* 31

TikTok, 'An Update on Fulfilling Our Commitments under the Digital Services Act' (*Newsroom | TikTok*, 16 August 2019) <<https://newsroom.tiktok.com/en-eu/fulfilling-commitments-dsa-update>> accessed 7 February 2025

——, 'Continuing to Protect the Integrity of TikTok during Romanian Elections' (*Newsroom | TikTok*, 6 December 2024) <<https://newsroom.tiktok.com/continuing-to-protect-the-integrity-of-tiktok-during-romanian-elections?lang=en-150>> accessed 27 October 2025

——, 'Community Guidelines: Overview' (*TikTok*) <<https://www.tiktok.com/community-guidelines/en/>> accessed 26 October 2025

——, ‘How TikTok Recommends Content’ (*tiktok.com*) <<https://support.tiktok.com/en/using-tiktok/exploring-videos/how-tiktok-recommends-content>> accessed 13 October 2025

Turillazzi A and others, ‘The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications’ <<https://papers.ssrn.com/abstract=4007389>> accessed 13 November 2024

Tushnet R, ‘Power Without Responsibility: Intermediaries and the First Amendment’ (2008) 76 *George Washington Law Review* 101 <<https://papers.ssrn.com/abstract=1205674>> accessed 21 November 2024

Uhlenbusch J, ‘Elon Musk, the Systemic Risk’ (*Verfassungsblog*, 7 February 2025) <<https://verfassungsblog.de/elon-musk-the-systemic-risk/>> accessed 7 February 2025

United States Department of Justice, ‘Department of Justice Wins Significant Remedies Against Google’ <<https://www.justice.gov/opa/pr/departement-justice-wins-significant-remedies-against-google>> accessed 15 September 2025

US Congress, ‘Moody v. NetChoice, LLC: The Supreme Court Addresses Facial Challenges to State Social Media Laws’ <<https://www.congress.gov/crs-product/LSB11224>> accessed 9 October 2025

Vermeulen M, ‘Researcher Access to Platform Data: European Developments’ (2022) 1 *Journal of Online Trust and Safety* <<https://tsjournal.org/index.php/jots/article/view/84>> accessed 23 May 2025

Vervaele JAE, *Compliance and Enforcement of European Community Law* (Wolters Kluwer 1999)

Vicinanza A, ‘La responsabilità delle piattaforme digitali nei confronti dei contenuti illegali: dal caso Telegram al Digital Services Act’ [2025] *Quaderni AISDUE* 195 <<https://www.aisdue.eu/anna-vicinanza-la-responsabilita-delle-piattaforme-digitali-nei-confronti-dei-contenuti-illegali-dal-caso-telegram-al-digital-services-act/>> accessed 3 March 2025

——, ‘Asymmetric National Enforcement Structures for EU Digital Rules: Can Cross-Border and Cross-Sector Cooperation Work?’ in Simona Demkova and Giovanni De Gregorio, *Enforcing the EU Digital Acquis* (The Digital Constitutionalist 2025) <<https://digi-con.org/enforcing-the-eu-digital-acquis/>> accessed 10 February 2026

——, ‘Il primo atto di enforcement del Digital Services Act tra tensioni geopolitiche: la sanzione della Commissione europea nei confronti di X (Twitter) –

AISDUE' (*Blog DUE*, 18 January 2026) <<https://www.aisdue.eu/anna-vicinanza-il-primo-atto-di-enforcement-del-digital-services-act-tra-tensioni-geopolitiche-la-sanzione-della-commissione-europea-nei-confronti-di-x-twitter/>> accessed 5 February 2026

Volokh E, 'Cheap Speech and What It Will Do' [1995] *Yale Law Journal* <<https://openyls.law.yale.edu/handle/20.500.13051/8884>> accessed 25 February 2025

Volokh E and Falk D, 'First Amendment Protection for Search Engine Search Results -- White Paper Commissioned by Google' (*Social Science Research Network*, 20 April 2012) <<https://papers.ssrn.com/abstract=2055364>> accessed 19 March 2025

von der Leyen U, 'A Union That Strives for More. My Agenda for Europe. Political Guidelines for the next European Commission 2019-2024' <https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en?filename=political-guidelines-next-commission_en.pdf>

Wax E, 'EU Tech Laws Imperilled by Friend and Foe' (*Euractiv*, 27 August 2025) <<https://www.euractiv.com/section/politics/news/eu-tech-law-imperilled-friend-for-capitals/>> accessed 27 August 2025

Wilman F, 'Between Preservation and Clarification. The Evolution of the DSA's Liability Rules in Light of the CJEU's Case Law.' in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023)

Wimmers J, 'The Out-of-Court Dispute Settlement Mechanism in the Digital Services Act: A Disservice to Its Own Goals' (2021) 12 *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law* 381 <<https://www.jipitec.eu/jipitec/article/view/332>> accessed 20 May 2025

Woolley K and Sharif MA, 'Down a Rabbit Hole: How Prior Media Consumption Shapes Subsequent Media Consumption' (2022) 59 *Journal of Marketing Research* 453 <<https://doi.org/10.1177/00222437211055403>> accessed 29 October 2025

Wu T, *The Master Switch: The Rise and Fall of Information Empires* (Faculty Books 2010) <<https://scholarship.law.columbia.edu/books/176>>

——, 'Is Filtering Censorship? The Second Free Speech Tradition' (*Brooking.edu*, 27 December 2010) <<https://www.brookings.edu/articles/is-filtering-censorship-the-second-free-speech-tradition/>> accessed 13 November 2024

——, 'Is the First Amendment Obsolete?' (2018) 117 *Michigan Law Review* 547 <<https://repository.law.umich.edu/mlr/vol117/iss3/4>>

Wu T and Thompson SA, 'The Roots of Big Tech Run Disturbingly Deep' *The New York Times* (7 June 2019) <<https://www.nytimes.com/interactive/2019/06/07/opinion/google-facebook-mergers-acquisitions-antitrust.html>, <https://www.nytimes.com/interactive/2019/06/07/opinion/google-facebook-mergers-acquisitions-antitrust.html>> accessed 24 June 2025

X, 'The X Rules: Safety, Privacy, Authenticity, and More' <<https://help.x.com/en/rules-and-policies/x-rules>> accessed 26 October 2025

York JC, 'Policing Content in the Quasi-Public Sphere' (*OpenNet Initiative*, 2010) <<https://opennet.net/policing-content-quasi-public-sphere>> accessed 23 December 2024

Younes R, 'Meta's Broken Promises' <<https://www.hrw.org/report/2023/12/21/metass-broken-promises/systemic-censorship-palestine-content-instagram-and>> accessed 25 March 2025

Zalando, 'Zalando: Zalando Files Legal Action against the European Commission to Contest Its Designation as a "Very Large Online Platform" as Defined by the Digital Services Act' (*Zalando Corporate*, 27 June 2023) <<https://corporate.zalando.com/en/company/zalando-files-legal-action-against-european-commission-contest-its-designation-very-large>> accessed 21 March 2025

Zara C, 'The Most Important Law in Tech Has a Problem' [2017] *Wired* <<https://www.wired.com/2017/01/the-most-important-law-in-tech-has-a-problem/>> accessed 7 January 2025

Zuboff S, *Il capitalismo della sorveglianza* (2023rd edn, Luiss University Press 2019)

Zuckerberg M, 'Building Global Community' (*Facebook*, 5 May 2021) <<https://www.facebook.com/notes/3707971095882612/>> accessed 4 March 2025

CASE-LAW

Google France SARL and Google Inc v Louis Vuitton Malletier SA [2009] Opinion Of Advocate General Poiares Maduro ECLI:EU:C:2009:569, C-236/08, C-237/08 and C-238/08

Google France SARL and Google Inc v Louis Vuitton Malletier SA [2010] Court of Justice of the European Union ECLI:EU:C:2010:159, C-236/08 to C-238/08

L'Oréal SA and Others v eBay International AG and Others [2010] Opinion of Advocate General Jääskinen ECLI:EU:C:2010:757, C-324/09

L'Oréal SA and Others v eBay International AG and Others [2011] Court of Justice of the European Union ECLI:EU:C:2011:474, C-324/09

Scarlet Extended SA v Sabam [2011] Court of Justice of the European Union ECLI:EU:C:2011:771, C-70/10

Sabam v Netlog [2012] Court of Justice of the European Union ECLI:EU:C:2012:85, C-360/10

Eva Glawischnig-Piesczek v Facebook Ireland Limited [2019] Opinion of Advocate General Szpunar ECLI:EU:C:2019:458, C-18/18

Eva Glawischnig-Piesczek v Facebook Ireland Limited [2019] Court of Justice of the European Union ECLI:EU:C:2019:821, C-18/18

YouTube and Cyando [2020] Opinion of Advocate General Saugmandsgaard Øe ECLI:EU:C:2020:586, C-682/18 and C-683/18

YouTube and Cyando [2021] Court of Justice of the European Union ECLI:EU:C:2021:503, C-682/18 and C-683/18

Meta platforms and Others [2023] Court of Justice of the European Union ECLI:EU:C:2022:704, C-252/21

Data Protection Commission v European Data Protection Board [2025] Court of Justice of the European Union ECLI:EU:T:2025:116, T-70/23, T-84/23 and T-111/23

Zalando v European Commission [2025] Court of Justice of the European Union, General Court ECLI:EU:T:2025:821, T-348/23

Meta Platforms Ireland v Commission [2025] Court of Justice of the European Union ECLI:EU:T:2025:842, T-55/24

Tiktok Technology v Commission [2025] Court of Justice of the European Union ECLI:EU:T:2025:843, T-58/24

Amazon Services Europe Sàrl v European Commission Order of the President of the General Court of 27 September 2023, Court of Justice of the European Union ECLI:EU:T:2023:589, Case T-367/23 R

Twitter, Inc v Taamneh [2023] Supreme Court of the United States 21–1496

Gonzalez v Google LLC [2023] Supreme Court of the United States 21–1333

Moody v Netchoice [2024] Supreme Court of the United States 22-277

APPENDIX

Figure 2. Instagram's option on each sponsored content, including 'why are you seeing this ad' (screenshot taken on February 6, 2025)

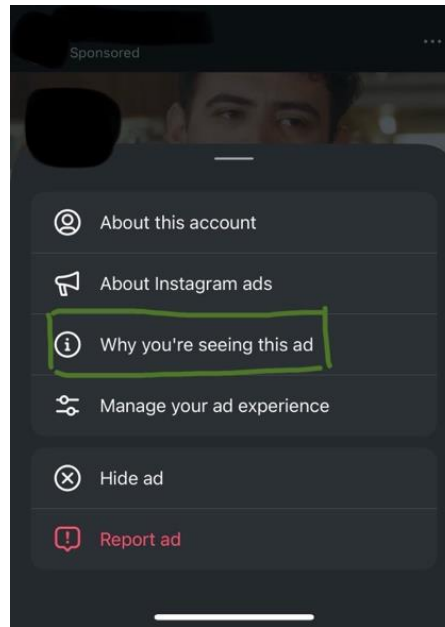


Figure 3. Explanation on 'why you're seeing this ad?' on Instagram: advertisers' choices and individual user's activity (screenshot taken on February 6, 2025)

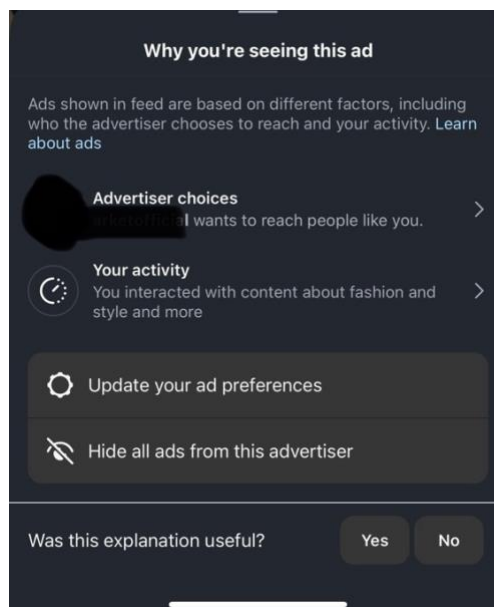


Figure 4. Explanation on ‘why you’re seeing this ad?’ on Instagram: the criteria selected by the advertiser to target the user (screenshot taken on February 6, 2025). This are the only targeting criteria for user who selected the less personalized version with ads breaks.

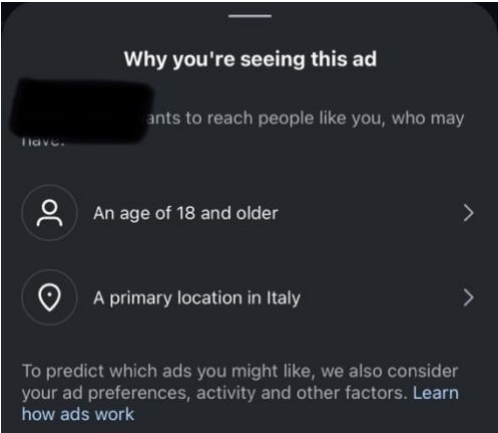


Figure 5. Explanation on ‘why you’re seeing this ad?’ on Instagram based on the user’s activity (screenshot taken on February 6, 2025). This category of targeting criteria only concern user who selected the more personalized version of the service without ads breaks.

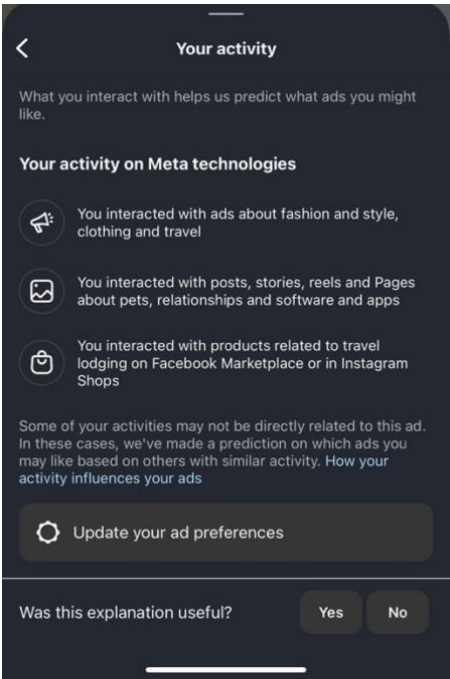


Figure 6. Pay or consent options (screenshot taken on February 13, 2025)

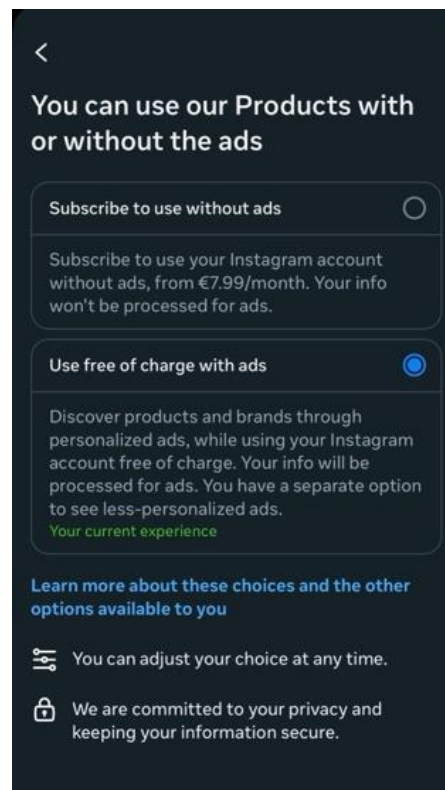


Figure 7. Different options for personalized advertisements on Instagram (screenshot taken on February 6, 2025)

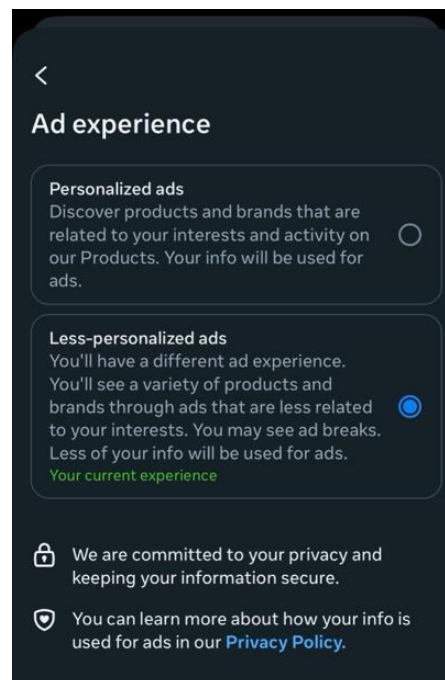


Figure 8. Gatekeeper designation under the DMA and overlaps with VLOP/VLOSE designation under the DSA

