Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

European Union Law Working Papers

No. 85

The EU's Digital Services Act and Its Impact on Online Platforms

Sebastian Kuclar Stiković

2024

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share "works in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Sebastian Kuclar Stiković has earned an LL.M. degree in European and International Business Law at the University of Vienna, Austria. Prior to that, he earned bachelor's and master's degrees in law from the University of Ljubljana, Slovenia. He has previously advised a software development company on data protection and privacy regulations. Currently, he is working as an in-house counsel for a joint-stock company, primarily in the field of contract law and M&A transactions. His main areas of interest include information technology law, intellectual property law and corporate law.

General Note about the Content

Suggested Citation

This European Union Law Working Paper should be cited as:
Sebastian Kuclar Stiković, The EU's Digital Services Act and Its Impact on Online Platforms, Stanford-Vienna European Union Law Working Paper No. 85, http://ttlf.stanford.edu.

Copyright

Abstract

On the 23rd of April 2022, the European Parliament and the Member States of the EU came to a political consensus regarding the proposal for the Digital Services Act (DSA), initially put forth by the European Commission in December 2020. Subsequently, this proposal received endorsement on the 5th of July 2022. On the 4th of October 2022, the Council of the European Union provided its definitive consent to the DSA Regulation. Mandatory obligations, enforceable across the EU, will be applicable to all digital services that facilitate consumer access to goods, services, or content. This includes the institution of new mechanisms for the rapid eradication of illegal content and the extensive safeguarding of the fundamental rights of users in the digital space. An additional objective is to fortify democratic governance and supervision of systemic platforms, as well as to diminish systemic perils such as manipulation or the spread of false information. The DSA elaborates upon the regulations set out in the e-Commerce Directive and confronts the challenges that have arisen in relation to online intermediaries. The regulatory approach to these services has varied among Member States, leading to obstacles for smaller enterprises aiming to broaden their reach across the EU and resulting in disparate levels of protection for European citizens. The new regulations will be enforced within the EU single market, including online intermediaries based outside the EU that provide services within the single market. Concurrently, online intermediaries will also profit from the definitive legal clarity regarding exemptions from liability, as well as from a harmonized set of regulations when offering their services in the EU. The paper aims to scrutinize the current regulatory framework and the regulations recently proposed, including the European Commission's strategy for establishing a uniform regulatory environment for internet companies within the European single market. It will evaluate how the new regulations to restrict the commerce and distribution of illegal goods, services, and content online will enhance the virtual experiences of EU residents and businesses, and it will discuss the necessity of these new rules. It seeks to provide insight into whether the Digital Services Act, with its mandate for access to platform data, furnishes the appropriate instruments to achieve its objectives. The DSA has the capacity to transform the internet and affect how the rights of individuals are honored online. The paper will explore how this transformation may unfold.

Table of Contents

1. Introduction

The market for digital content is global, open to development and in a state of constant change and growth. This not only presents economic prospects for firms that can engage with this marketplace, but also provides society with an abundance of advantages, such as the freedom of information, cross-cultural interaction, and a diverse range of options for media content consumption, despite the risks and challenges inherent in such a globalised exchange. 'Intermediaries and other platforms that enable or provide access to content, collect and categorise content, provide forums for sharing and user creation of content are regularly the gatekeepers to these benefits.'[1]

Digitisation and the internet make communication easier, but they also make it easier to restrict or abuse freedom of expression and harder to resist these practises. The establishment of digital platforms that serve as a medium of communication has created a gap in terms of the tools to protect freedom of expression on the one hand and from abuse of the right by those who exercise it on the other.[2] Users are no longer just passive recipients of content, but rather content creators who present themselves with diverse offers on various platforms in text, image, video or sound. As a negative consequence, there is now easy access to illegal content, content that incites hatred, terrorist propaganda and disinformation.[3]

An asymmetrical distribution of power is also evident in the new digital world. The internet was seen as a place of freedom, as it was assumed that after the exclusion of public power, there was no more room for private power. However, this romantic notion proved to be wrong

---

[1] Mark D. Cole, Christina Etteldorf and Carsten Ullrich, *Updating the Rules for Online Content Dissemination: Legislative Options of the European Union and the Digital Services Act Proposal* (Nomos Verlag 2021) 17.
[2] Jerzy Menkes, 'Freedom of Speech in the Age of Digitalisation: Opportunities and Threats' in Lukasz Dawid Dąbrowski and Magdalena Suska (eds), *The European Union Digital Single Market: Europe's Digital Transformation* (Taylor & Francis Group 2022) 36-37.
[3] Cole, Etteldorf and Ullrich (n 1) 76-77.

when web governance changed drastically: from a web consisting of atomistic and decentralised actors to a highly centralised system in which virtual networks and communities are centrally controlled by large web actors. Rules that were established, contracted with and enforced by actors to run their businesses, e.g. the terms of use of platforms, became governance guidelines, e.g. on what content and users are allowed on social networks. In legal terms, these are contractual rules between users and providers, and rules governing relationships between users that they voluntarily accept by signing up for a service and thereby giving their free and informed consent. In essence, these are 'community rules' established in a context of pervasive asymmetric bargaining, market and social power, where platforms have the concrete ability to define and enforce their ToS, which constitute what is called 'platform law'.[4] That is, platforms are not the recipient but the source of law: 'a rule-maker in a private legal order'.[5]

Digital platforms play a crucial role in today's economy, have a wide range of different activities, and offer enormous potential for growth and wealth creation. Some of them have reached enormous size in terms of customers, revenue, market capitalization, and unprecedented economic and social importance. These platforms compete in global markets, connect a very large and growing number of users, and interact with a wide variety of businesses, ranging from traditional communications and media players to small, specialised companies.

In the early stages of their development, digital platforms embodied the positive side of an unregulated world in which laissez-faire policies left 'checks and balances' to the market. This approach led to a) the pro-competitive entry of new, innovative and efficient players into

[4] Antonio Manganelli and Antonio Nicita, *Regulating Digital Markets: The European Approach* (Springer International Publishing 2022) 78-79.
[5] ibid 78-79.

monopolistic or oligopolistic markets (such as the media and news markets, wholesaling, bookselling, taxi services, etc.) and/or b) the creation of new products, services and markets. This disruption of 'traditional' markets, companies and business models has long been perceived as positive by end users and also by policy makers, including antitrust authorities around the world.[6]

Online platforms, including those known as 'gatekeepers', are now increasingly taking on the role of primary custodians of the social, scientific, and political content they disseminate, as well as the virtual spaces where merchants and consumers interact. Gatekeepers are substantial tech firms that create and oversee the platforms and the regulations for business affiliates and consumers within an internet platform model, and they amass data, the digital market's most prized asset. Owing to their magnitude, they possess a colossal market superiority relative to their rivals. Diminished competition and inequitable practices in the digital domain are issues that are more prevalent and more acute in certain digital services than in others. This applies in particular to widespread and widely used digital services and digital infrastructures, which usually mediate directly between business customers and end customers.[7]

An acceleration of the policy debate on the regulation of digital markets occurred when it became clear that a soft policy approach to protecting innovation must be balanced against the risk that unregulated markets and companies could lead to excessive, perhaps permanent, concentration of market power and potentially consumer harm.[8]

In the EU, the core liberties set out in the Treaty on the Functioning of the European Union (TFEU) are vital to the fulfilment of the EU's internal market, which encompasses the digital

---

[6] ibid 26.
[7] Adam A. Ambroziak, 'EU's Perspective on the Functioning of Giant Online Platforms in the Digital Economy' in Lukasz Dawid Dąbrowski and Magdalena Suska (eds), *The European Union Digital Single Market: Europe's Digital Transformation* (Taylor & Francis Group 2022) 5.
[8] Manganelli and Nicita (n 4) 11-12.

arena, aptly termed by the Commission as the 'Digital Single Market'. The free movement of goods, the right of establishment, and the liberty to offer services are principally designed to maintain market openness and provide legal certainty to economic agents within these markets. In essence, companies ought to have the capacity to distribute their merchandise and services freely across the EU and to establish operations in any member state without facing discrimination or barriers from the host country. Regarding the cross-border spread of online content, this applies not just to media corporations that benefit from these freedoms, but also to all entities engaged in content distribution. Exceptions to fundamental freedoms, whether at national or EU level, must be justified by an objective of general interest and the measures taken to achieve this objective must be proportionate.[9]

Two legal acts were recently passed in the legislative process in the EU. The first is the Regulation on a Single Market for Digital Services (Digital Services Act – DSA)[10]. The DSA aims to ensure a safe and responsible online environment. This Act also aims to improve mechanisms for the removal of illegal content and the effective protection of users' fundamental rights online, including freedom of speech. The second is the Regulation on contestable and fair markets in the digital sector (Digital Markets Act – DMA)[11]. It sets out competition-based *ex ante* rules for large online platforms that can act as 'gatekeepers', setting the 'rules of the game' for their users and competitors.[12]

The DSA aims to modernise the current legal framework for digital services with clear rules defining the responsibilities of digital services to address the risks faced by their users and

[9] Cole, Etteldorf and Ullrich (n 1) 83.
[10] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.
[11] 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) [2022] OJ L265/1.
[12] Cole, Etteldorf and Ullrich (n 1) 79.

protect their rights. It sets out a number of fundamental rules and principles for the way intermediaries are involved in the distribution of content online, it also contains important new rights for users and obligations for service providers in areas such as content removal, complaint handling mechanisms and out-of-court dispute resolution.[13] The DSA extends and updates the key principles set out in the e-Commerce Directive[14] adopted in 2000 (and still in force today) and sets the legal framework for the provision of digital services in the EU by defining clear responsibilities and accountabilities for providers of intermediary services according to their role, size and impact in the digital ecosystem.[15]

2. Digital space in the EU and its challenges

Prior to the DSA, digital services were regulated at the European level by the e-Commerce Directive, which was a regulatory response to the problems that arose in 2000 and is therefore somewhat outdated. This directive is mainly aimed at removing barriers to cross-border online services in the EU and creating legal certainty for operating in the digital economy. The scope of the e-Commerce Directive on the digital economy is broad and covers both B2C and B2B transactions as well as 'free services', i.e. services financed by advertising and sponsorship.[16] Also prior to DSA, the EU had already introduced exceptions to the e-Commerce Directive in two legal instruments: The Audio-visual Media Services Directive (AVMSD)[17], which

[13] Joan Barata and others, *Unravelling the Digital Services Act Package* (European Audiovisual Observatory 2021) 20.
[14] 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') [2000] OJ L178/1.
[15] Manganelli and Nicita (n 4) 187.
[16] ibid 57.
[17] 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) [2010] OJ L95/1; Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [2018] OJ L303/69.

extended the scope of the Directive to video-sharing platforms (VSPs), and the Directive on Copyright in the Internal Market (DSM)[18], which introduced new obligations for online content-sharing platforms (OCSPs).[19] The AVMSD in particular is an essential component of the relevant legal framework for the dissemination of online content, despite the minimum harmonisation approach it pursues. Particularly noteworthy are the rules for video-sharing platforms adopted with the 2018 revision, which place greater obligations on this type of platform provider because they are seen as part of the audio-visual media landscape and must therefore be subject to at least similar rules as other media services in order to protect recipients.[20]

The e-Commerce Directive established a particular regime of liability for online intermediary services, with four principal goals: 1. to distribute the responsibility for maintaining a secure internet among all private entities involved and to enhance cooperation with public authorities – for instance, parties who have been wronged should notify online platforms of any illegal activities they detect and such platforms ought to eliminate or restrict access to unlawful content of which they become aware; 2. to ensure that the internet remains a safe and secure environment, promoting the expansion of e-commerce across Europe by certifying that online platforms are not compelled to scrutinise the legality of all content they host; 3. to achieve an equilibrium among the basic rights of the various parties concerned, particularly the safeguarding of privacy and freedom of speech, the freedom to conduct business (for the platforms), and the right to property, which includes the intellectual property rights of those who are harmed; and 4. to consolidate the Digital Single Market by embracing a shared EU

[18] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L130/92.
[19] Barata and others (n 13) 1.
[20] Cole, Etteldorf and Ullrich (n 1) 22.

criterion for exemptions from liability, particularly at a juncture when national regulations and judicial decisions are progressively diverging.[21]

The main principles of the e-Commerce Directive are the freedom to provide online services (Article 3), and the freedom of establishment of online service providers in EU territory (Article 4). The freedom to provide services in the EU Member States is enshrined in the internal market clause, which also ensures that online service providers are subject to the law of the Member State in which they are established and not to the law of the Member States in which the service is accessible ('Country of Origin' principle). Member States may not restrict the freedom to provide online services unless such measures are necessary to protect public health, public security, or consumer protection. These measures must be proportionate and notified to the EU Commission, which will check their compatibility with EU law.

In order to strive for a trustworthy online environment, the e-Commerce Directive lays down harmonised rules concerning transparency and information requirements for online service providers (Article 5), commercial communications (Article 6), electronic contracts (Article 9 et seq.) and limitations of liability for providers of intermediary services (Article 12 et seq.). The general legal principle is that ISPs can only be held liable if they have some form of 'control' over the content and information. In particular, the Directive provides for a generally applicable system of specific exclusions of liability based on the activity carried out by the ISPs: a) mere conduit (Article 12), b) caching (Article 13) and c) hosting (Article 14). Directive intentionally exempts Internet Service Providers (ISPs) from the obligation to check and monitor all information flowing through their networks, as such an obligation would be

[21] Barata and others (n 13) 24-25.

impossible or too burdensome for ISPs (Article 15). However, they are obliged to report cases of suspected illegal activity to the competent authorities.[22]

Under the e-Commerce Directive, the host provider is required to act 'expeditiously' to withdraw or block access to unlawful content once 'actual knowledge' of 'illegal content or activities' is acquired. This method has several identified weaknesses. For one, there is no clarification on what constitutes 'Illegal activities', nor is there an explanation of 'actual knowledge'. Furthermore, there are substantial variances in both the definition and the operation of notice-and-takedown across the EU. Member States have instituted diverse frameworks, including a 'notice and takedown' system where illegal content must be eliminated; a 'notice and stay down' system, meaning illegal content must be eradicated and prevented from re-uploading; and a 'notice and notice system', where the hosting provider is only expected to pass on the notice of infringement to the purported infringer. Some Member States have not established any notice and takedown procedures at all. This diversity of models throughout the EU results in significant legal ambiguity for internet intermediaries. Moreover, the e-Commerce Directive does not standardise the procedural protections, and merely a handful of Member States have introduced 'counter-notice' processes allowing individuals to contest a demand to remove purportedly unlawful material.[23]

Rather than initiating an overhaul of the e-Commerce Directive, the Commission opted to create specialised tools to tackle particular types of unlawful content. Consequently, in recent times, sector-specific legislation has been enacted to enhance the responsibilities of online intermediaries. Not only are the ECD and media-specific secondary legislation pertinent to the spread of online content, but also additional sector-specific rules that, for instance,

[22] Manganelli and Nicita (n 4) 58-59.
[23] Tambiama Madiega, *Reform of the EU Liability Regime for Online Intermediaries: Background on the Forthcoming Digital Services Act* (European Parliamentary Research Service 2020) 6.

predominantly aim at economic or consumer protection policy goals. The Digital Single Market Directive (DSMD) delineates a new class of 'online content-sharing service provider' and imposes entirely novel responsibilities upon them; the Platform-to-Business Regulation mandates specific informational and transparency duties for online intermediary services and search engines that influence the visibility of content and products. Existing directives such as the General Data Protection Regulation (GDPR)[24], with its highly harmonising approach based on the marketplace principle, and Regulation on the Dissemination of Terrorist Content Online (TERREG)[25] are as significant for the online or platform domain as those presently debated. In addition, there are instruments that deliberately allow leeway and exemptions for the pursuit of media and cultural policy objectives at the national level, which enable supplementary rules concerning content dissemination. This is supplemented by a number of measures to promote self-regulation at the level of EU coordination and support measures, e.g. in the area of hate speech and disinformation. Overlaps with the horizontal rules of the ECD are inevitable. These secondary legal bases not only need to be reconciled with new legal bases or those that need to be reformed, but also show that there are and must be special rules for certain information society service providers, aimed at specific objectives and particularities.[26]

2.1. Exception to the national liability regime

Under the ECD, a hosting platform can be exempted from liability for illegal material uploaded by users if it has 'no actual knowledge of illegal activity or information (…) and no knowledge of facts or circumstances from which the illegal activity or information is apparent'. If the platform has such knowledge or awareness, it can only invoke immunity from liability if it

[24] 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) [2016] OJ L119/1.
[25] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance) [2021] OJ L172/79.
[26] Cole, Etteldorf and Ullrich (n 1) 22.

'acts expeditiously to remove or disable access to the information'. All types of illegal content or activities are covered (unfair market practises, violation of data protection rules, damage to honour and reputation, etc.) as well as different types of liability (criminal or civil). The hosting platform should also be neutral in the sense that its behaviour is 'purely technical, automatic and passive, indicating that it does not know or control the data it stores' (CJEU).[27] The difference between 'active role' and 'passive role' could be clarified for a range of new activities including distribution and processing of third-party data, networking, collaboration, matchmaking, indexation and ranking services under the EU liability regime.[28] The concept of liability is intertwined with the concept of knowledge. In this context, not only is the intermediary entitled to ignore the content, but any legislation that would oblige the intermediary to generally monitor the content would be incompatible with EU law under Article 15 of the Directive. Although Article 14 does not explicitly refer to or even mention a reporting system as mandatory, the second requirement of the article does not allow for a different interpretation: the intermediary is only eligible for immunity from fines if it provides the user with a mechanism to alert him to a specific instance of illegal content.[29]

Some recently adopted sector-specific legislation at EU level seems to contain new obligations regarding the adoption of proactive measures. In this sense, the Copyright Directive contains a number of obligations towards the online content sharing service providers (OCSSPs), in particular to ensure the unavailability of certain works protected by copyright (Article 17) and to prevent their further upload.[30] It imposes stringent obligations on online service providers whose main purpose is to store and provide public access to a large amount of copyright protected works. The recently adopted Regulation on addressing the dissemination of terrorist

[27] Barata and others (n 13) 25.
[28] Madiega (n 23) 14.
[29] Philippe Jougleux, *Facebook and the (EU) Law: How the Social Network Reshaped the Legal Framework* (Springer International Publishing 2022) 161.
[30] Barata and others (n 13) 11-13.

content online (TERREG) contains important obligations for hosting service providers in relation to the removal of illegal content and the introduction of specific measures to combat the distribution of terrorist content online.

Even if no general monitoring obligations may be imposed, OCSSPs are free – also in line with Article 7 of the DSA – to carry out general monitoring on their own initiative, in any case respecting Article 17(7) and (9) of the Copyright Directive as well as the principle of proportionality and the users' right to freedom of expression and information, which is also protected by Article 11 of the EU Charter of Fundamental Rights.

From the copyright perspective, Article 17 of the Copyright Directive indirectly affects the safe harbour, as the intermediary is liable if it has not acted with extreme diligence to ensure the unavailability of certain works for which the rightsholders have provided a list. The immunity of the intermediary concerns liability for illegal content, not liability for non-compliance with an administrative or judicial order. Every time the 'safe harbour' takes a step back, even indirectly, questions arise about the protection of freedom of expression. The Court has explicitly addressed this issue by adding a safeguard to the mechanism of injunctions against intermediaries. It must be ensured that the measures taken to comply with the injunction do not unnecessarily deprive internet users of lawful access to the information available.[31]

In a certain sense, the two immunity provisions mentioned above exhibit a certain internal tension. On the one hand, the first immunity from liability (for third-party content) upholds the notion that digital platforms constitute a neutral environment, a kind of open public sphere for online discussions, in which the platform merely acts as an intermediary without playing a role in the type of content delivered. On the other hand, the option for platforms to moderate content

[31] Jougleux (n 29) 178.

according to their terms of use without being held liable for it provides for a policy that, at least in some respects, violates the above-mentioned assumption of mere conduit, i.e. neutrality of platforms in the provision of content.[32]

As regards the liability regime for providers of intermediary services, the e-Commerce Directive was adopted without taking into account today's powerful and dynamic platforms. This is why these provisions, which are so important for the functioning of the digital market society, were revised in order to better respond to their evolution. Digital Services Act contains rules for online intermediary services that are differentiated according to the role of the intermediary, its size and its influence on the digital ecosystem, and is a logical progression of the regulatory action launched ten years ago and 'clearly marks the end of the independence of cyberspace'.[33]

2.2. Data collection

Owing to the vast quantity of individuals using the internet, the extensive duration of their online engagement, and the immense volume of digital transactions, platforms amass an extraordinarily substantial trove of user data. This accumulation of data empowers the algorithms of these platforms to construct detailed profiles of individual service and product demand for each user, in terms of preferences, requirements, and spending propensity. The platforms utilise this profiling to generate revenue from the data, either by directly engaging in online retail or indirectly through the acquisition of targeted, customised advertising. Furthermore, through the examination of fresh data, algorithms are progressively refined, enhancing their predictions regarding user preferences and, consequently, the precision of profiling. This mechanism permits platforms to amplify their capacity for matching, thereby

[32] Manganelli and Nicita (n 4) 170-71.
[33] Barata and others (n 13) 34.

increasing demand from both segments of the market: for users, by boosting the efficiency and quality of services (that is, services or products more closely aligned with users' predilections and necessities), and for the other group (such as advertisers), by expanding the number or the concentration of users targeted by advertisements. All these factors present compelling motives for platforms to gather an ever-expanding corpus of data by employing 'zero price' business strategies and broadening the scope and extent of their operations.[34]

The data available to technology companies can be used to optimise product offerings, adapt advertising and multimedia communication, predict consumer behaviour and tailor products to consumers' expectations or (sometimes artificially created) needs. Another way to benefit from the data discovered in recent years is to use it to develop services based on artificial intelligence. These services, once customised, will be offered to other companies. Consequently, the ability to derive value from data increasingly determines the competitive position on the market. It is therefore about the value that online platforms create in online commerce not only in the form of material goods and services, but also about big data — large, variable and diverse data sets.[35]

These detailed data profiles are what render polarisation on social networks particularly perilous. The algorithms favour material that sparks negative feelings like fear and anger. Such detailed profiles of users allow for intense personalisation; that is, each individual is shown precisely the content that deeply affects them. This highly customised polarisation captivates people and holds their attention to the screens. It is at this juncture that the DSA intervenes. It delves deeper than just the surface issues, casting a discerning eye on the actual roots of these significant democratic threats: hatred, provocation, disinformation, and surveillance. Beneath

[34] Manganelli and Nicita (n 4) 122-23.
[35] Ambroziak (n 7) 11.

the surface of its abstract language lie tangible instruments designed to uncover the algorithms that promote hateful content and false information, consequently muddying the waters of public discourse. The DSA establishes the foundation for the exacting analysis necessary for legislators and regulators to forge evidence-based policy and precise regulations for an internet where the voice of every individual can be heard.[36]

2.3. Algorithmic decision making

Owing to their gatekeeping roles, intermediaries and platforms can either enable or impede access to the online arenas where public discourse is increasingly taking place. Intermediaries that possess search or recommendation functionalities, typically governed by algorithms, wield extensive sway over the availability, accessibility, visibility, retrievability, and prominence of specific content. This impact is partly exerted through the deployment of algorithmic personalisation (or recommendation systems).[37]

The proliferation of information sources has augmented so-called 'external pluralism' – the diversity resulting from myriad competing information outlets – and broadened the scope of freedom of expression. This applies both to the freedom to disseminate information and the freedom to educate oneself by evaluating varying alternative sources. Within this framework, every individual can craft their own unique 'broadcasting' or 'newspaper' online.[38] Nevertheless, this tremendous growth in the volume of information accessible on the Internet leads to the dilemma of 'information overload', that is, a surfeit of information that overwhelms consumers and obstructs their informed decision-making. How does one sift through the ocean of decentralised information to pinpoint 'relevant' content?[39] For this purpose, algorithmic

[36] Alexandra Geese, 'Why the DSA Could Save Us From the Rise of Authoritarian Regimes' in Joris van Hoboken and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023) 71-72.
[37] Barata and others (n 13) 45.
[38] Manganelli and Nicita (n 4) 173.
[39] ibid 23.

information sources are employed to navigate through the digital deluge of information and to effectively identify pertinent information by precisely discerning and aligning with consumers' (present) preferences for informative content.

This is where the role of the platforms' algorithms becomes crucial. In traditional media markets, the reputation and brand loyalty of the main newspapers, radio and television stations act as selection mechanisms for information providers, which viewers implicitly entrust with the selection of information and content. There, viewers selected competing content by freely choosing between competing editorial offerings. On the Internet, this selection mechanism is mainly carried out by the platforms' algorithms: The data revealed by users enables the creation of algorithm profiles to select the content that is most likely to be requested by individual user. This means that while platform users make a free and informed choice, they do so in an information environment that is deliberately designed, tailored and selected by algorithms. Since there is too much information on the supply side, this algorithmic selection process reduces the time that would otherwise be needed to evaluate, philtre and finally select potential content. Algorithms therefore minimise transaction costs on the online information market. It is the flood of information that makes the work of algorithms efficient and useful. The algorithms of the platforms also undertake an additional role: as users engage with particular 'selected' material and manifest their preferences, the algorithm proffers 'suggestions' for additional content that may capture the interest of users. This feature is associated with the flip side of the digital exchange, namely micro-targeted advertising, which has the objective of reaching potential consumers. This necessitates the creation of what is known as 'stickiness' or 'engagement' – the imperative for the platform and its remunerating clients in the online advertising sphere to keep drawing the attention of users. Consequently, the algorithmic curation of content is transformed into a multifaceted, perpetual process with the overarching aim of amplifying the duration users spend on the platform, thereby maximising value for the

advertisers involved in the exchange. This procedure is unequivocally far from being 'neutral', both in the method by which information and data are amassed and in the manner in which content is structured and presented to users.[40]

Reducing transaction and search costs also reduces the time consumers spend searching for information. However, this inevitably undermines pluralism, as algorithmic product efficiency allows consumers to receive only the information they would like to receive, i.e. their own existing representation of the world. Efficient 'content' matching, especially in search engines and social networks, has the unintended consequence that content that is not 'likeable' or does not fit the current user profile virtually disappears from the user's information sphere. As more and more citizens in Europe and around the world inform themselves through search engines and social networks, the 'efficient algorithmic matching' of digital platforms is raising growing concerns about the nature and extent of online pluralism. At the same time, disinformation and misinformation strategies have succeeded in spreading falsehoods during the elections and in the context of the COVID-19 pandemic. This process is observed as the formation of digital echo chambers and the polarisation of citizens, which could ultimately have a major negative impact on fundamental aspects of society and political systems. The consequences are in most cases unintended by the platforms, which have also developed and established internal policy governance to correct socially undesirable outcomes. However, this outcome is inherently linked to their specific business model, which is applied by platforms to all types of products, including information.[41]

The algorithmic system that assures an effective liaison between content creators and consumers on one side, and platforms with advertisers on the other, forms the essence of the

[40] ibid 173-74.
[41] ibid 23-24.

digital exchange. The business strategies of the platforms hinge on user 'lock-in' or engagement – that is, the platform's ability to hold users' attention, measured by the time spent engaging with the platform's content. This is commonly achieved through the 'suggestion' of related content. Since these domains are delineated by algorithmic profiling shaped by 'big data', the analysis of digital service design still refers to three distinctive aspects of the digital transaction:: 1. the side of content seekers, whose freedom to choose content is constrained by the choices 'suggested' by algorithms according to the preferences revealed by users' digital footprints; 2. the content producers' side, whose freedom to reach content seekers is controlled by the platforms' algorithms; 3. the advertisers' side, whose freedom to bring content producers and content seekers together is managed and monetised by the platforms' algorithms.[42]

The influence of the algorithm is not limited to the mere experience on the platform, this hierarchisation of information has an impact on users' daily lives. It has the power to positively or negatively influence the feelings of its users in a specific geographical area. The vast collection of personal data available to the platform enables it to carry out microtargeting, i.e. to precisely exploit a user's feelings. These feelings are determined or even predicted on the basis of a personality analysis. It is argued that by analysing just 300 'likes' and other reactions from users, Facebook is able to accurately determine their personality. Furthermore, the algorithm has some obvious implications for democratic societies. While the link between the filtering effect of the algorithm and the global rise of populism has not yet been proven, the suspicion of a possible connection is growing louder, and more and more studies are pointing to it. For example, a correlation has been found between the number of anti-refugee posts on far-right Facebook pages in Germany and the number of hate crimes over the same period.[43] Additionally, it has also been said that the algorithm as a philtre bubble (or polarisation

[42] ibid 172.
[43] Jougleux (n 29) 234-35.

amplifier) inherently undermines our ability to think collectively about our problem. 'Although it is not intended to do so, the algorithm operates de facto as a form of moderation: by choosing what type of content appears first and assuming that most of users do not check half of their feed, it actually determines what content will be visible and what content will be shadow banned.'[44]

3. Protection of users' fundamental rights

3.1. Freedom of speech definition

'Freedom of speech is one of the four freedoms'[45] — an individual liberty intimately entwined with political entitlements. It was heralded as an instrument of defiance against totalitarian rule for the realisation of fundamental human rights and democracy. It is instrumental in actualising the right to democratic governance and adherence to the rule of law, and it delineates the expanse of human liberty to select a religion and belief, conduct scientific inquiries, and engage in artistic creation.[46] 'Freedom of speech constitutes one of the essential foundations of such a society, one of the basic conditions for its progress and the development of every man.'[47] Freedom of speech is a negative right; this means that the government cannot, by law, take action against the person exercising this freedom.

This freedom also embodies a positive aspect. The state is mandated to shield freedom of speech from illegitimate encroachments by private entities on others' exercise of this liberty, as governed by the horizontal effect of laws. Furthermore, the state is compelled to enact positive measures, that is, to implement provisions for the unimpeded dissemination of information and

[44] ibid 235.
[45] Franklin Roosevelt, 'The Four Freedoms' <https://www.archives.gov/milestone-documents/president-franklin-roosevelts-annual-message-to-congress> accessed 20 November 2023.
[46] Menkes (n 2) 35.
[47] *Handyside v The United Kingdom* (1976) Series A no 24.

ideas ('direct' positive action).[48] The European Court of Human Rights (ECtHR) employs a tripartite test in adjudicating disputes concerning freedom of speech: Any restriction must be stipulated by law and conform to the necessary standards of precision and accessibility; it must pursue a legitimate goal as per Article 10(2) of the European Convention on Human Rights and be 'necessary in a democratic society'.

Digitisation has vastly expanded the avenues for 'speech' and reduced the hurdles to the exchange of human communication and ideas. The right to freedom of speech encompasses the liberty to maintain opinions (free from intrusion) and to seek, receive and disseminate information and ideas across any medium, including the Internet, irrespective of frontiers. Digital technology has introduced a novel instrument to the array of communicative technologies without supplementing the means to exercise free speech. In scenarios where the law curtails state actions, platforms have assumed the role of arbiters of speech (a status enabled by judicial decisions affirming platforms' rights to exclude individuals from their services).[49] Facebook, Twitter, Instagram, and YouTube consistently remove posts that transgress their standards on violence, sexual content, privacy, and the like. These platforms also frequently restrict numerous users or specific subjects. Twitter, in particular, highlights posts that feature misleading or controversial assertions.

Regarding the legal parameters for the transnational broadcast of online content, fundamental freedoms, as enshrined in the Charter of Fundamental Rights of the EU (CFR), the European Convention on Human Rights of the Council of Europe (ECHR), and the stipulations of domestic constitutional legislation, provide the cornerstone and scaffold for any resolution. These rights underscore human dignity, which, according to the CFR, is 'inviolable', that is, it

[48] Menkes (n 2) 35.
[49] ibid 36-37.

must be acknowledged as the paramount aim of safeguarding. This also encompasses the protection of minors for their benefit. Conversely, the freedom of expression (pertaining to both service users who generate content and those who receive it) and the rights of service providers, who may be subject to amplified legal responsibilities, must be upheld. Within the remit of protecting fundamental rights, the competences of Member States in the realm of media regulation and the preservation of diversity must be observed, particularly in relation to platforms that position themselves as arbiters of media access.[50]

3.2. Freedom of speech history

Freedom of speech has been enshrined in legal documents that lay the foundations for human rights and establish a global norm for them. These documents include: The 'Act Declaring the Rights and Liberties of the Subject and Settling the Succession of the Crown',[51] which asserts that 'freedom of speech and debates or proceedings in Parliament ought not to be impeached or questioned in any court or place out of Parliament'; the 'Declaration of the Rights of Man and of the Citizen',[52] which proclaims in Article XI: 'The free communication of ideas and opinions is one of the most precious rights of man: every citizen may, therefore, speak, write, and print freely, subject to the responsibility for the abuse of this freedom in cases determined by law'; and the First Amendment to the Constitution of the United States, which is a part of the Bill of Rights[53] and states that 'Congress shall make no law (…) prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press'.

Following World War II, nations proclaimed at the United Nations General Assembly their commitment to 'universal respect for and observance of human rights', including 'freedom of

[50] Cole, Etteldorf and Ullrich (n 1) 21.
[51] Bill of Rights 1689.
[52] Déclaration des droits de l'Homme et du citoyen 1789.
[53] United States Bill of Rights 1791.

speech'. During its first session, the General Assembly of the UN asserted that 'Freedom of information is a fundamental human right and the touchstone of all the freedoms to which the United Nations is dedicated'[54]. This principle was later enshrined in the Universal Declaration of Human Rights (Article 19): 'Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers'[55]. Article 19's provision was expanded in Article 19 of the International Covenant on Civil and Political Rights:

> 1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other medium of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.[56]

3.3. Freedom of speech in the EU

Freedom of speech and the legal structure for its realisation within Europe are articulated in Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms:

---

[54] UNGA Res 59 (14 December 1946) UN Doc A/RES/59(1) para 1.
[55] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR).
[56] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), art 19.

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial wholeness or public safety, for the prevention of disorder or crime, for the safeguarding of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for upholding the authority and impartiality of the judiciary.[57]

Examining the legal parameters governing the cross-border spread of online content, the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union (CFR), the European Convention on Human Rights of the Council of Europe (ECHR), and the tenets of national constitutional law must underpin and inform any approach adopted. Paramount among these rights is human dignity, which, as per the CFR, is deemed 'inviolable', meaning it must be upheld as a paramount objective safeguarded by state actions. In the context of online content, there are numerous potential infringements upon the rights of individuals, notably attacks on human dignity. This is particularly pertinent to audio-visual materials featuring certain types of pornography or violent imagery. With non-fictional depictions, an assault on dignity may be inferred when an individual is presented as a mere 'object'. Similarly, specific fictional content might be considered an infringement under certain circumstances.[58]

---

[57] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).
[58] Cole, Etteldorf and Ullrich (n 1) 81.

Justifying any encroachment upon fundamental rights and freedoms essentially requires a delicate balancing of competing interests, where these competing interests may also be protected under fundamental rights or freedoms. The more severe and immediate the risk to a legal right, the more defensible it becomes to endorse robust state interventions by citing other legal interests. As a result of a nuanced proportionality assessment, it follows that certain market players carry more substantial and stringent responsibilities than others. Pertaining to the dissemination of online content, for instance, content intermediaries have a distinct function compared to other platforms and face greater risks concerning the aforementioned fundamental rights. Given the significance of such platforms in distributing and making media and communication content accessible at large, it stands to reason that they warrant specific scrutiny during the overhaul of the horizontally applicable regulations for information society services.[59]

3.4. Freedom of speech and the DSA

Regulating online discourse poses significant challenges in terms of fundamental rights, encompassing the freedom of expression, anti-discrimination, and the entitlement to an effective legal remedy. This becomes acutely complex with regards to 'lawful but awful' expressions like disinformation, which carry broader consequences for the public sphere or the democratic process. Firstly, the Digital Services Act (DSA) enforces stricter obligations on Very Large Online Platforms (VLOPs) — those with a user base exceeding 45 million or 10% of the EU populace — due to their expansive influence and the potential to amplify harm. Secondly, the strategy employed is holistic, being both preventive and responsive, directive yet adaptable. VLOPs must detect, lessen, and report systemic risks on their platforms, but are afforded a degree of leeway in this mandate. Lastly, the risk-centred approach is discerning,

[59] ibid 83.

targeting not just (external) systemic risks but also the influence of (internal) operational models and design choices.[60]

All intermediaries encompassed by the regulation (bar micro-enterprises) would be obliged to submit annual reports of their content regulation efforts. These must detail the number of content removal demands from national bodies, user notifications or flags, the speed of their responses, and an elaborate summary of actions they have initiated themselves regarding content management and complaint resolution. For online platforms, the requirements tighten, necessitating reports on all automated content regulation processes, including their objectives, accuracy metrics, and any implemented protective measures. Very large online platforms (VLOPs) are subject to even more rigorous standards, being required to issue transparency reports biannually.

Moreover, every digital intermediary within the scope (technical intermediaries, hosting services, online platforms, and VLOPs) must explicitly inform users in their terms of service of any usage limitations, including policies on content moderation and specifically those involving algorithmic decisions and human oversight. Furthermore, when imposing restrictions, service providers are expected to act with diligence, objectivity, and proportionality, duly considering the rights and legitimate interests of all involved parties in line with relevant fundamental rights.

The DSA introduces a safeguard against abuse of the notification system. According to Article 23(2), the right of a user, individual, or legal person who frequently submits manifestly unfounded notifications or complaints could be temporarily suspended from the notification process (after prior warning). The regulation aims to ensure transparency at every step of the

[60] Barata and others (n 13) 59.

process. Article 15 states that providers of intermediary services shall publish, at least once a year, clear, easily understandable, and detailed reports on the content moderation they have carried out during the period in question.

3.5. Access to justice and to an effective remedy in the DSA

Access to justice is not an independent right. It is a concept that encompasses a number of core human rights[61], such as the right to a fair trial (Article 6 ECHR; and Article 47 Charter of Fundamental Rights of the EU, CFREU), and the right to an effective remedy (Article 13 ECHR and Article 47 CFREU). These are primarily procedural rights that oblige states to organise domestic procedures in order to ensure better protection of rights. To a certain extent, they serve as instruments that help to maximise the effectiveness of substantive rights such as the right to freedom of expression, the right to privacy and reputation, freedom of assembly or freedom of thought.[62]

The right to a fair trial encompasses numerous components, one of which is procedural fairness. This concept pertains to the conduct of legal proceedings as opposed to their conclusion. The DSA aims to ensure procedural fairness by enhancing the clarity and foreseeability of proceedings through its comprehensive stipulations on notice and action (for instance, Articles 16-23). The legislation frequently refers to the right to an effective remedy and a fair trial. Specifically, Article 17 and Recitals 39, 52, 55, and 59 highlight that the explanations provided in Article 17 ought to deliver clear, comprehensible, precise, and specific information concerning the remedies available, enabling affected individuals to actually avail themselves of these remedies. Recital 39 underlines the obligation for Member States, in applying the DSA,

[61] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European law relating to access to justice* (Publications Office of the European Union 2016).
[62] Aleksandra Kuczerawy, 'Remedying Overremoval' in Joris van Hoboken and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023) 170-71.

to honour the fundamental right to an effective remedy and a fair trial, as stipulated in Article 47 of the Charter of Fundamental Rights of the European Union (CFREU).

Within the realm of online expression, the right to an effective remedy is invoked on two distinct occasions. Initially, when an individual affected by an offending expression seeks to halt it, for instance by demanding its deletion. Subsequently, when the originator, following a successful deletion, seeks to contest this action and calls for the reinstatement of the expression.[63] Platforms are obliged to process complaints in a timely, non-discriminatory, diligent, and non-arbitrary manner – as stipulated in Article 20(4). It is mandated that resolutions to complaints should not rely solely on automated processes and that decisions should be overseen by suitably qualified personnel – as per Article 20(6). Upon addressing a complaint, platforms are required to notify the involved parties of their substantiated decision without unreasonable delay. They must also provide details regarding the option for out-of-court dispute settlement as outlined in Article 21, along with other accessible remedial measures – referenced in Article 20(5). The Digital Services Act (DSA) should not obstruct the capacity of national judicial or administrative bodies to issue orders for the restoration of content that adheres to the conditions but was erroneously deemed illegal and removed. Recital 59 further notes that the facility to contest decisions made by online platforms should not preclude the pursuit of judicial remedies.

Does this imply that the DSA is effectively advocating for a right to a forum and compelling platforms to host all content that is not unlawful? Such an assertion would be excessively expansive. Moreover, this is not the intended purpose of the DSA. Platforms retain the discretion to define within their terms and conditions the content they disallow, subject to the constraints in Article 14 (due consideration for freedom of expression, media freedom,

[63] ibid 174-75.

pluralism, and other fundamental rights and freedoms). It is anticipated that they will become more stringent and explicit in enumerating all undesirable content, also as a repercussion of the transparency obligations of Article 14.[64] This would also align them with recent legal precedents, such as those in Germany[65], where the judiciary has commenced instructing the reinstatement of content that contravenes vaguely formulated terms and conditions but is not illegal.

3.6. Hate speech online

The characterisation of hate speech as a criminal act has evolved under various international and EU influences. In 1948, the United Nations General Assembly enacted the crime of incitement to genocide. The International Convention on the Elimination of All Forms of Racial Discrimination of 1965 suggested making illegal the spread of ideas rooted in racial superiority or hate, the incitement to racial discrimination, and all forms of violence or incitement to such violence against any race or group of people of another colour or ethnic background, including the endorsement and funding of racist activities. The International Covenant on Civil and Political Rights from 1966 further refines 'hate speech' by detailing the fundamental components of the offence: the range of protected characteristics is limited and definitive (encompassing national, racial, or religious hatred); it necessitates 'advocacy', meaning a deliberate and public endorsement of hatred; the 'hatred' promoted must lead to incitement of discrimination, hostility, or violence, that is, illicit tangible actions.[66]

In 2012, a tentative conciliation entitled the 'Rabat Plan of Action' was adopted, which contains a six-part threshold test for forms of speech that are prohibited under criminal law. The test takes particular account of the elements of incitement to hatred, the speaker, the intent, the

[64] ibid 175-76.
[65] See Bundesgerichtshof III ZR 179/20 and III ZR 192/20.
[66] Jougleux (n 29) 184.

content, the extent of the speech and the likelihood of causing harm. The 'Rabat Plan' is therefore an important guide for the courts when assessing the legality of content.[67]

'Unlike the United States, the EU does not view the right to hate speech as a valuable part of public discourse. Instead, the EU views hate speech as a harmful manifestation of discrimination.'[68] While the EU has instituted a stringent legal structure regarding hate speech, it has embraced a collaborative and non-mandatory method for overseeing hate speech on the internet. In 2016, the European Commission entered into a voluntary agreement with four American tech companies to tackle illegal hate speech online: Facebook, Twitter, YouTube, and Microsoft. This Code of Conduct obliges the signatory companies to create and uphold 'rules or community guidelines' that mirror the European criteria for hate speech.[69]

Council Framework Decision[70] provides that each Member State shall take the necessary measures to ensure that the following intentional conduct is punishable: public incitement to violence or hatred directed against a group of persons defined by reference to race, colour, religion, descent or national or ethnic origin, or a member of such a group. Therefore, the criminal offence of hate speech at EU level is defined by four elements: discrimination against a group of persons on the basis of a closed list of criteria defining these persons, an intention, an act of public communication and damage which is the potential consequence of incitement to violence or hatred against these persons. The first element is to be interpreted differently depending on the type of discrimination.[71]

---

[67] ibid 185.
[68] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2020) 159.
[69] ibid 166.
[70] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law [2008] OJ L328/55.
[71] Jougleux (n 29) 185-86.

In 2018 the European Commission against Racism and Intolerance (ECRI) had denounced the rise of incitement to racial hatred and the phenomenon of xenophobic populism, as well as their impact on the political climate in Europe. In the 2018 report, which was later confirmed in 2019, ECRI emphasised that 'citizens' growing fears about the economic situation and geopolitical and technological changes' were being exploited 'by those who use migrants and minorities as scapegoats, and in particular by populist politicians who aim to divide societies on national, ethnic and religious lines'. This practise, ECRI emphasised, is 'not only pursued by fringe political groups, but has also become increasingly prevalent in the more traditional parties and national governments - a phenomenon of great concern'. Online hate speech is often fuelled by the spread of falsehoods or 'strategies' of misinformation.[72]

Recent reforms in Europe have endeavoured to tackle the issue of online pluralism. In Germany, the NetzDG[73] legislation was enforced in January 2018, compelling operators of social networks to delete material that is manifestly identified as hate speech within 24 hours of a report, while material that is more contentious has up to seven days to be removed. Non-compliance with the statute may result in a fine of as much as 50 million euros. In France, a statute targeting the spread of false information and online defamation[74] was enacted in November 2018. In the three months preceding an election, electoral candidates may present an objection to the judiciary against statements deemed false or slanderous to secure their expedient removal. Offenders may face up to a year's imprisonment and a penalty of as much as 75,000 euros. Furthermore, the grievance can be filed by a public entity, political party, or any individual claiming to have been harmed. Media outlets that broadcast illicit news are required to reveal the identities of their backers or advertisers.[75]

---

[72] Manganelli and Nicita (n 4) 187.
[73] Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl I S 3352).
[74] loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.
[75] Manganelli and Nicita (n 4) 185.

Currently, the EU legislator is acting through the Digital Services Act (DSA), which will necessitate online platforms to adopt stricter policies. Specifically, Article 23, titled 'Measures and protection against misuse', prescribes in detail the suitability of sanctions enacted by the online platform. Article 23(1) mandates that online platforms should, after issuing a prior warning, suspend their services for a reasonable period for users who consistently post manifestly illegal content. Article 23(4) imposes a duty on online platforms to enhance their transparency. The platform is required to explicitly and comprehensively outline in its terms and conditions its policy regarding the misuse outlined in paragraphs 1 and 2, including the facts and circumstances considered in determining whether behaviour constitutes abuse and the timeframe for the suspension.

3.7. Fake news

In practice, fake news is often inextricably linked with hate speech and can be seen as a means to achieve the latter's ends. The propagation of fake news on social networks frequently ignites incitement to hatred. Both phenomena yield similar outcomes: fake news compromises the right to factual information and thus endangers democratic societies. However, conflating the two phenomena would be erroneous since they differ in key aspects. Unlike hate speech, fake news does not inherently incite violence. Hate speech constitutes a recognised and measurable threat; conversely, fake news is amplified by novel technological advancements, casting uncertainty on its future trajectory. The EU's inaction can partly be attributed to the belief that fake news does not immediately challenge the union's core values and the relatively recent emergence of the 'fake news epidemic'. Differing from hate speech, at the EU level, fake news has not been specifically categorised as a criminal offence.[76]

[76] Jougleux (n 29) 194-95.

To be considered fake news, it must only be objective information (news), not opinions, and this information must be proven to be false from a scientific point of view. Furthermore, it is only possible to criminalise fake news if the fake news has a real impact on society. And finally, in order to criminalise fake news, criminal intent would have to be proven, which requires the perpetrator is aware of the falsity of the information in the first place.[77]

3.8. Disinformation strategies

Disinformation strategies are far more intricate than mere fake news, involving deliberate intent, recurrence, systematic planning, and either virality or targeting specific individuals for economic and/or political ends. False information, which might seem credible, is purposefully fabricated to damage a person, social group, organisation, or nation, or to bolster/disparage, with conscious distribution for political, ideological, or commercial motives, including click baiting. This encompasses a) false context, where genuine content is combined with fabricated information; b) fraudulently influenced content, spread by sham sources or fake profiles masquerading as legitimate ones; c) entirely concocted content, created from scratch to mislead and/or cause harm; and d) manipulated news, where factual information or images are intentionally and deceitfully altered. A disinformation scheme is crafted to be convincing to the recipient, who inadvertently informs the algorithm of his interests through his data profile. The algorithmic curation of online content, based on user profiles, delivers personalised narratives, essentially the specific type (dis)information that users 'want and need'.[78]

In December 2018, the European Commission initiated an action plan to enhance collaboration among Member States and EU bodies in combating disinformation threats, particularly in anticipation of the 2019 European elections. Facebook, Google, Twitter, and Mozilla

[77] ibid 196.
[78] Manganelli and Nicita (n 4) 178-79.

voluntarily pledged to the Code of Practice on Disinformation in October 2018, agreeing to: a) impede revenue from advertisements on web profiles or sites that manipulate information and supply advertisers with sufficient security and data concerning websites propagating disinformation; b) endorse the distribution of political advertising messages to the populace and participate in more principled advertising practices; c) maintain a transparent and public strategy on identity and online automation, and act to remove counterfeit profiles; d) offer resources and information to assist individuals in making informed decisions and facilitate access to a variety of viewpoints regarding matters of public interest, giving precedence to credible sources; e) grant researchers entry to data that adheres to privacy standards so they can monitor and more comprehensively understand the proliferation and influence of disinformation.[79]

Self-regulation has encountered a number of shortcomings. It is essential to investigate the connection between the content, the account, and the advertising to identify offending or suspect entities that exploit disinformation and/or clickbait tactics. However, a challenge that emerges is the inefficacy of self-regulation when it is not rigorously monitored by independent authorities that possess the capability to inspect and audit, specifically concerning data and algorithms, to ascertain the efficacy of the actions implemented.[80]

4. What are online platforms?

Online platforms serve as multi-sided intermediaries across various sectors, employing distinct business models (such as social media, search engines, creative content outlets, app distribution services, communication services, payment systems, and platforms for the sharing economy). By amplifying economies of scale and scope, along with indirect and direct network

[79] ibid 186.
[80] ibid.

externalities, there tends to be an escalation in market concentration within the digital sphere. Often these markets are prone to a phenomenon referred to as 'tipping': once an online platform achieves critical mass (the tipping point), its expansion becomes self-reinforcing due to network effects and the costs users incur when leaving the platform, leading to the continual growth of its user base, potentially resulting in a monopolistic single operator. This situation is described as 'winner-takes-all', as platform costs increase linearly with user numbers, yet revenues tend to surge exponentially.[81]

Online platforms are a trading and communication channel alongside the traditional one, a new type of market where supply and demand meet. As Kenney and Zysman have noted,[82] online platforms can be seen as a complex mix of software, hardware, operations and network. They give a broad group of users access to a combination of techniques, technologies and interfaces that can build what they want on a solid foundation. The platforms set the rules of the game and binding standards, which can reduce transaction costs; they provide suitable tools (e.g. a browser) and services (e.g. payment systems) and can use the data available to them to bring the transaction sides together according to certain criteria. Online platforms are therefore based on a 'complete business model that integrates demand and supply, that is, market creation, establishing, or facilitation using new technologies'.[83]

The notion of the business model referenced above warrants scrutiny because its innovative character is frequently cited to justify certain practices by major online platforms, which may at times be perceived as anti-competitive. Certain academics explicitly argue that what is at hand is not merely a business model but rather a comprehensive business ecosystem. This represents the most sophisticated form of a business network currently in existence, comprising

[81] ibid 118-22.
[82] Martin Kenney and John Zysman, 'The Rise of the Platform Economy' (2016) 32 Issues in Science and Technology 61-69.
[83] Ambroziak (n 7) 7.

a highly interconnected array of organisations, stakeholders, and consumers engaged in exchange, production, innovation, commerce, collaboration, and communication, all co-evolving towards a mutual aim or around a pivotal organisation.[84] Furthermore, online platforms are acknowledged as digital infrastructures that supply essential functionalities, enabling third-party entities to connect and interact. This interaction facilitates the provision of complementary products and services and executes diverse roles, often congregating interdependent groups within multi-sided markets.[85]

In principle, online platforms offer the same services as in the analogue world; they bring business partners and consumers together. However, two points should be considered: the type of services and the data. According to the currently binding EU rules,[86] the above-mentioned services provided by online platforms are so-called information society services, i.e. services that (a) are provided for remuneration, which is the basic requirement for identifying a service covered by the rules on the free movement of services and the internal market; (b) are provided at a distance, i.e. without the simultaneous presence of the service provider; (c) by electronic means (using electronic devices) and at the individual request of the recipient of the service (which excludes action on the initiative of the service providers). It should be noted that the platforms offer a variety of services, the scope of which is greater than currently provided for in the regulations, including the part offered free of charge by consumers to attract their attention. In this way, they subsidise access to them, for example, in order to maximise profits in other areas of activity.[87] There are over 10,000 online platforms operating in Europe's digital

[84] Diana Moss, Greg Gundlach and Riley Krotz, 'Market Power and Digital Business Ecosystems: Assessing the Impact of Economic and Business Complexity on Competition Analysis and Remedies' SSRN Electronic Journal <https://ssrn.com/abstract=3864481> accessed 15 December 2023.
[85] Ambroziak (n 7) 7-8.
[86] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L241/1.
[87] Ambroziak (n 7) 8.

economy, most of which are small or medium-sized enterprises. However, only a small number of very large online platforms account for a very large share of the digital economy in the EU. These platforms have become de facto gatekeepers between businesses and citizens as consumers.[88]

5. The new Regulation on a Single Market for Digital Services

5.1. Regulation vs. Directive

When it comes to obligatory legal measures, there typically exists a choice between regulations and directives if the legal foundations refer broadly to actions. The principal distinction resides in the legal character of these two types of legal acts: A regulation is immediately enforceable across all member states and thus generally holds supremacy over national legislation within its field of application. On the other hand, directives require transposition into the domestic law of the member states. Hence, in instances of overlap, the regulation also takes precedence over the directive or its national enactment. This distinction consequently leads to various benefits and drawbacks associated with each legal instrument.

Beyond the inherent constraints posed by opting for a regulation as the most binding tool on the legislative and executive capacities of the Member States, there are several more nuanced issues. When the proposed new act must integrate into an intricate weave of existing sectoral regulatory frameworks at both EU and national levels (with Member States retaining significant powers due to connections with media regulation and possessing entitlements to various exemptions and powers to derogate under sectoral legislation), the level of harmonisation envisioned in a horizontal regulatory framework must be carefully evaluated. Three principles should be observed: Regulations inherently have priority (both in principle

[88] Aida Ponce Del Castillo, 'The Digital Services Act package: Reflections on the EU Commission's policy options' (2020) 12 ETUI Policy Brief 2.

and in legal conflicts) over (intersecting) directives and national laws within their realm of applicability; more contemporary legislation generally supersedes older statutes; and more specific laws have precedence over more general ones. To preclude legal ambiguity, any newly enacted legal instrument must explicitly address all these considerations. This is already proving difficult in the area of cross-border dissemination of online content, for which there is a complex bundle of interlocking rules not only of a media-specific nature but also of a general economic nature due to the diversity of the players involved and the distribution channels and reception options. In addition, the EU's clear ban on harmonisation in the cultural sector (Article 167(5) TFEU) must also be carefully considered. This necessity becomes all the more relevant when a set of rules is not limited to a (horizontal) regulation of a large number of online players with some basic elements of a framework – as was the case with the ECD, where problems in relation to sectoral EU and national law had become apparent – but contains very specific and extensive regulations.[89]

5.2. European Commission's Proposal

According to the Commission, the main objective of the DSA package is to improve the functioning of the internal market and fair competition. The language used by the Commission is centred around 'trading practises', 'market competition', 'fragmentation' and 'asymmetries'.[90] For the Digital Services Act (DSA) proposal, the Commission has chosen the legal foundation of Article 114 of the Treaty on the Functioning of the European Union (TFEU), which permits the development of measures that underpin the establishment or operation of the internal market. In terms of the requisite harmonisation and its scope, the Commission recognises that barriers to economic activities stem from disparities in the formulation of national laws. This is evidenced by the fact that certain Member States have enacted or are

[89] Cole, Etteldorf and Ullrich (n 1) 119-20.
[90] Castillo (n 88) 5.

considering enacting legislation pertaining to subjects such as the removal of illegal content online, due diligence responsibilities, notification and action mechanisms, and the transparency of platform providers.[91]

Concerning the principle of subsidiarity, the Commission mentions in the supporting document to the Digital Services Act (DSA) proposal that the internet is inherently transnational and that legislative attempts at the national level, as mentioned previously, obstruct the offering and receipt of services throughout the European Union and are inadequate in providing safety and uniform safeguarding of the rights of Union citizens and enterprises online. In its impact assessment, the Commission notes that 'a patchy framework of national rules jeopardises an effective exercise of the freedom of establishment and the freedom to provide services in the EU' and thus deduces that this issue cannot be resolved through national measures. From the Commission's standpoint, this challenge can only be addressed by regulation at the Union level, as it believes that only measures at this level can ensure predictability and legal certainty, diminish compliance costs throughout the Union, while also promoting equal protection for all Union citizens and ensuring a coherent approach for intermediary service providers operating in all Member States.[92]

The nature and extent of the obligations under the Digital Services Act (DSA) will be determined by the type and size of the platform in question. 'Intermediary services' is employed as an umbrella term encompassing 'mere conduit', 'caching', and 'hosting'. These are further broken down in terms of exemption from liability (once more into caching, mere conduit, and hosting as per the e-Commerce Directive) and the establishment of obligations (for hosting providers, online platforms, and very large online platforms), with certain

[91] Cole, Etteldorf and Ullrich (n 1) 134.
[92] ibid 134-35.

allowances for micro and small enterprises. The DSA's territorial reach is predicated on the establishment principle, meaning the rules apply to any intermediary service offered to recipients established or resident in the Union, regardless of the service provider's location. Provision of a service within the Union implies a 'substantial connection with the Union', which particularly refers to having an establishment in the Union, a significant user base, or targeting activities towards the internal market. New duties introduced include labelling requirements for illicit goods, services, and content, the creation of user complaint mechanisms, and enhanced transparency obligations. However, the DSA also seeks to bolster internet law enforcement and, to this end, proposes novel supervisory structures intended to function effectively in cross-border scenarios.

Very large online platforms are subject to additional regulations to curtail the systemic risks associated with the spread of illegal content via their services. These risks range from potential adverse impacts on the exercise of certain fundamental rights, such as respect for private and family life and freedom of expression and information, to the intentional manipulation of their services. Specifically, such platforms are required to conduct an annual assessment of the systemic risks related to their operations and usage within the EU and implement suitable and effective measures to mitigate these risks. A crucial element of the proposal concerning the employment of self-learning algorithms mandates that the key parameters of the decision-making algorithms, which determine content presentation on the platforms (the ranking mechanism), be made transparent. Moreover, platforms must present users with at least one alternative that does not rely on profiling.[93]

The proposal mandates that the very large platforms grant access to pertinent data to the Digital Service Coordinator (appointed by each Member State as the primary enforcer) or to the

[93] Manganelli and Nicita (n 4) 191-92.

Commission itself to verify adherence to the DSA provisions. Such data, within specified limits and conditions, must also be made available to academic researchers for the purpose of systemic risk studies. The DSA sets out particular stipulations for the intensified oversight of large online platforms if they fail to fulfil these responsibilities. Additionally, should there be repeated non-compliance, the European Commission is authorised to step in.

The reasons for the tougher regulatory approach are probably twofold. Firstly, the severity and frequency of controversies related to illegal online content has reduced public confidence in the self-regulation of IT companies. Secondly, the decision by some large Member States — including France, Germany and the UK — to introduce national legislation to combat hate speech online has given the Commission a strong rationale for acting in the internal market, as it wants to prevent inconsistent national legislation from emerging in different Member States.[94]

5.3. e-Commerce Directive vs Digital Services Act Regulation

In contrast to its predecessor, the e-Commerce Directive, the DSA defines illegal content in Article 3(h) with a broad definition:

> [I]legal content means any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law.[95]

The classification of intermediary service providers remains as it was. The DSA encapsulates this classification by introducing a definition for intermediary services in Article 3(g), encompassing the trio of established categories: mere conduit, caching services, and hosting

[94] Bradford (n 68) 163.
[95] Digital Services Act, art 3.

providers, while explicitly confining the term to these categories. The descriptions of these three categories in Articles 4, 5, and 6 of the DSA are virtually identical to those in Articles 12(1), 13(1), and 14(1) of the e-Commerce Directive (ECD). The DSA consequently extracts these definitions from the conditional exemptions from liability found in the ECD, where they were previously only mentioned. Thus, a hosting service is distinctly articulated in Article 3(g) as a 'service consisting of the storage of information provided by, and at the request of, a recipient of the service'. However, this is merely a consolidated expression, as it lays the groundwork for the liability exemption rule for hosting providers outlined in Article 6 of the DSA. For instance, Recital 17 of the DSA declares that the rules of the DSA do not create a positive basis for liability. Hence, non-compliance with the conditions for liability exclusion does not automatically render the intermediary service provider liable. The existence of such liability must be determined independently following the relevant EU law or national law provisions.[96] The tolerable level of passiveness depends on the intermediaries' roles. This principle is already established by the European Court of Justice's ruling in the Google France case.[97] Intermediaries such as 'mere conduit' service providers and 'caching' providers have mostly a passive role and no or limited knowledge about the user content they convey, to the contrary, 'hosting providers' play a more active role, with more control over the content they host. They are subsequently subject to more stringent 'duties of care' and 'notice and take down' obligations.[98] Recital 17 also clarifies that the exclusions of liability in the DSA apply to any type of liability and to any type of illegal content. Recital 28 takes into account the increasing diversity of different types of intermediaries, in particular those that intervene at the infrastructure level to improve the transmission and storage of data in the increasingly complex

[96] 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 and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023) 37-38.
[97] Case C-236/08 *Google France SARL and Google Inc. v Louis Vuitton Malletier SA* [2010] ECR I-02417, para 107.
[98] Madiega (n 23) 3.

and congested internet system. The recital opens up the possibility that new services or services that were not previously focussed on as intermediary services are covered by liability protection: content delivery networks, internet registries, messaging services, digital certificate authorities or voice over IP services are mentioned, among others. The recital emphasises that the liability exemptions only apply if they actually fulfil all the criteria of one of the three categories.[99]

There is the special provision in Article 6(3) DSA on the liability under consumer protection law of certain types of hosting service providers, namely online platforms that enable consumers to conclude distance contracts with traders (in simple terms: B2C online marketplaces).[100] This regulation takes into account the previous case law of the ECJ, in particular Wathelet.[101]

The proposal leaves the current system of largely reactive safe harbour conditions unchanged but adds clarifications on liability conditions in relation to voluntary own-initiative obligations (Article 7), the prohibition of general monitoring obligations (Article 8) and reactive obligations in relation to authority orders to act against illegal content (Article 9) and to disclose information (Article 10). Article 7 introduces a 'good Samaritan clause' which ensures that the exemptions from liability continue to apply to those providers who carry out voluntary investigations on their own initiative and take measures aimed at detecting, identifying and removing illegal content in order to fulfil the requirements of Union law, which would include the expectations set out in the DSA.[102] Voluntary own-initiative investigations or other activities aimed at detecting, identifying and removing illegal content or disabling access to it,

[99] Cole, Etteldorf and Ullrich (n 1) 163-64.
[100] Wilman (n 96) 39.
[101] Case C-149/15 *Sabrina Wathelet v Garage Bietheres & Fils SPRL* [2016] EU:C:2016:840.
[102] Cole, Etteldorf and Ullrich (n 1) 173.

or taking the necessary measures to fulfil the requirements of Union law, do not mean that the intermediary has lost its 'passive role'.[103]

Despite the provisions in Article 8, Articles 9 and 10 establish additional prerequisites for exemption from liability. Firstly, intermediary service providers are required to promptly respond to orders pertaining to particular illegal content and to swiftly notify the issuing authorities of the actions taken and the dates thereof. For these orders to be valid, they must be well-reasoned, include the URL(s) and, if necessary, other specific information to identify the content, as well as details of the redress available to both the provider and the service recipient (the uploader). The orders must also define their territorial reach, be in the language specified by the service provider, and be sent to the service provider's designated contact point, as outlined in Article 11. This is subject to the procedural rules of criminal law at the national and EU levels, further explicated in Recitals 31 to 36. Secondly, Article 10 mandates that providers must comply with requests to disclose certain details about one or more individual service recipients (users). These enquiries must also meet specific criteria: They should provide a rationale for the request and the remedies accessible; the provider should not be compelled to furnish information beyond what has already been gathered as part of their service; and the request should be in the declared language of the provider. Recital 37 distinctly precludes requests for aggregated data intended for statistical or policy-formulation purposes. It further clarifies that providers must adhere to injunctions against illegal content and to demands for data from any competent national or judicial authority in the EU, irrespective of whether the authority is located outside the provider's country of establishment. These stipulations are among the reasons why the DSA proposal includes provisions on the substance and procedure of these orders (Recitals 31-34) and elucidates their territorial scope (Recital 36).[104] Service

[103] Jougleux (n 29) 180.
[104] Cole, Etteldorf and Ullrich (n 1) 174-75.

providers should be able to process these orders effectively and efficiently and not be subject to different formats and procedural rules.

The fact that new obligations to respond to authority orders in relation to illegal content and to information orders have been added as a basic condition for the availability of the liability exemptions (in Articles 9 and 10) demonstrates the need to enable courts and authorities to require timely and consistent responses, especially in urgent cases. It is certainly an important development that national authorities can now issue orders directly to service providers, regardless of where they are based in the EU. This is in the interests of timely removal and information in a fast-moving area where the risks posed by the cross-platform distribution of illegal content can increase exponentially over time. Importantly, these obligations are without prejudice to sectoral provisions, such as the one-hour response time to removal orders provided for in the TERREG (Recital 34) or the relevant national legislation (Recital 31). It will certainly be interesting to see how authorities will assess whether content that is illegal in their jurisdiction is also illegal in other Member States, as stated in Recital 36. However, this is not a question of the liability exemption regime, but a question of regulatory co-operation (see below) and a welcome addition to enable more effective cross-border enforcement of the law.[105] Article 10 of the DSA concerning information orders fulfils a critical request from authorities and other concerned parties by delineating the conditions under which intermediaries are held accountable for unlawful user content, should they fail to reveal the user's identity to regulatory bodies for necessary action. The extension of these liability exemptions to all intermediaries is positively acknowledged, as it recognises that technical services like Internet Service Providers (ISPs), despite not being the principal focus of enforcement against the spread of illegal content, may nonetheless be subject to measures executed by the competent authorities.

[105] ibid 177-78.

Under the DSA, which extends the provisions of the ECD, all providers of intermediary services with an establishment within the EU are mandated to establish 'Single Points of Contact' (SPoC) that national authorities, the Commission, and the newly formed European Board for Digital Services can reach electronically (Article 11). Details on how to contact the SPoC must be readily accessible to the public. Intermediary service providers without an establishment in the EU are required to designate a legal representative in one of the Member States where they offer their services (Article 13). This legal representative takes on the role of the SPoC and may also face liability for any breach of the new legislation. Providers are obliged to notify the Digital Services Coordinator (DSC) of the name, physical address, email address, and telephone number of their legal representative in the Member State where the representative is located.

All providers of intermediary services must specify in their general terms and conditions the information/content restrictions they impose on users (Article 14). These restrictions should include a reference to content moderation policies, procedures and tools (including the use of algorithmic decision-making and human review). This information must be provided in 'clear and unambiguous language' and in an easily accessible format. In addition, providers are required to apply these policies and measures carefully, objectively and proportionately, taking particular care to ensure that they respect the fundamental rights principles of the EU Charter of Fundamental Rights.[106]

Intermediary service providers are required to release transparency reports concerning their content moderation practices annually, as stated in Article 15. These reports must encompass statistics on the orders received to counteract illegal content and information requested by the authorities (in line with Articles 9 and 10), the volume of orders sorted by the type of illegal

[106] ibid 189.

content, the grounds for intervention (be it the service terms and conditions or the applicable legislation), and the time needed to give effect to the order. Additionally, providers are obligated to disclose the quantity and classification of voluntary decisions made concerning the visibility, availability, and accessibility of content. The reports should also include a detailed account of complaints regarding content decisions, along with figures on the reinstatement of content (or the reversal of initial decisions). However, micro and small enterprises are exempt from this requirement.

The DSA corrects one of the main problems of the e-Commerce Directive, namely the lack of precision and transparency in relation to the notice and take down procedure. Article 16 of the DSA clarifies that the mechanism is mandatory and that it 'should be easily accessible and user-friendly and allow the submission of notices exclusively by electronic means'. It also stipulates that the notice must contain mandatory elements: an explanation of the reasons why the individual or legal person considers the information in question to be illegal content; a clear indication of the electronic location of that information; the name and an email address of the individual or legal person submitting the notice, except in the case of information deemed to concern one of the offences referred to in Articles 3 to 7 of Directive 2011/93/EU (offences related to child exploitation and child pornography); and a statement confirming that the natural or legal person submitting the report has a good faith belief that the information and allegations contained therein are accurate and complete. It could be argued that the procedure for warning and removing content under the DSA has developed into a quasi-judicial procedure. The author of the allegedly illegal content is informed in detail through a statement of reasons for moderation (Article 17). In addition, two appeal systems are established, one internal (Article 20) and one external, through out-of-court dispute resolution involving a certified out-of-court dispute settlement body (Article 21). Both the complainant and the author of the message are entitled to use these mechanisms and both can be subject to sanctions in the event of abuse (e.g.

repeated unfounded notices or repeated posting of illegal content), consisting first of a warning and then the suspension of the possibility to post or report content (Article 23).[107]

Recital 16 explains that the DSA aims to maintain the framework for the liability of intermediaries from the ECD, but also to clarify certain elements taking into account the case law of the CJEU. This article analyses the balance that the EU legislator has attempted to strike between these two considerations, i.e. preservation and clarification. In particular, it focuses on the impact of the ECJ's case law in relation to the ECD intermediary liability framework.[108]

6. New rules for removal of illegal goods, services or content online

6.1. Illegal content

According to the 2018 Eurobarometer survey, 61% of EU citizens say they have come across illegal content online and 65% believe that the internet is not safe to use. New measures called for by consumers to improve this situation include: a) more transparency in content moderation rules; b) more information about adverts to understand who sponsored the ad and how and why it targets a particular user; c) clearer information about why a particular piece of content is recommended to users; d) the right for users to opt out of content recommendation based on profiling; e) better access to data for authorities and researchers to better understand online virality and its impact in order to reduce societal risks. As a result, many digital platforms have decided to introduce self-regulatory measures (codes of conduct), including (some of) the remedies mentioned above, to counteract illegal content. Nevertheless, much remains to be done to enable simple and clear reporting of illegal content, goods or services on online

[107] Jougleux (n 29) 180.
[108] Wilman (n 96) 37.

platforms and to create transparency in the implementation of the codes of conduct by the platforms.[109]

Regarding the content neutrality of its concept, the DSA imposes no specific limitations on particular types of content. Instead, it frequently uses the impartial term 'content' (e.g., 'content moderation', 'illegal content'). With respect to what content falls under the DSA's proposed obligations, the Regulation leans on a broad definition of illegal content that references Union or national law. By this formal definition, illegal content encompasses any information which, either by its very nature or through its connection to an activity, including the sale of products or the provision of services, fails to conform with Union legislation or the law of any Member State, without concern for the specific subject matter or nature of said law. Recital 12 of the DSA clarifies that this term, regardless of its manifestation, pertains to information that is illicit under the applicable law, such as illegal hate speech, terrorist content, and unlawful discriminatory content, or that is associated with activities involving illegal content, like the dissemination of images of child sexual abuse, the illegal, non-consensual sharing of private images, online harassment, selling non-compliant or counterfeit products, unauthorised use of copyrighted material, or activities breaching consumer protection statutes. It is crucial that hosting providers are permitted to conduct their own good faith evaluations based on the principles of legality, necessity, and proportionality, which, notably, are not explicitly articulated in the document.[110]

There is a general agreement among stakeholders that 'harmful' (yet not, or at least not necessarily, illegal) content should not be defined in the Digital Services Act and should not be subject to removal obligations, as this is a delicate area with severe implications for the

[109] Manganelli and Nicita (n 4) 168-69.
[110] Barata and others (n 13) 15-16.

protection of freedom of expression.[111] This category of 'lawful but awful' speech exists in some form in every legal system that conforms to human rights. The DSA has chosen not to regulate such speech directly by imposing new content bans that platforms must enforce, but instead to regulate the systems and processes by which platforms enforce their own community guidelines or other speech rules.[112]

Illegal content includes all information that does not comply with EU or national law, regardless of the precise subject matter or nature of that law. A distinction must be made between content that: a) violates EU or Member State law and is therefore illegal under the DSA definition; b) does not violate any law, but violates the terms and conditions of the platform on which it is posted; and c) does not violate any law or the terms and conditions of the platform, but causes harm to users, especially the most vulnerable (e.g. minors).[113]

It is important to note that the DSA does not standardise the definition of illegal content, be it products or services; it standardises only the procedural aspects. What constitutes illegal content is determined by existing laws at either the European or national level. The Commission's decision to refrain from directly regulating illegal content is understandable, given the complex balancing act required. Policymakers in the Member States have long grappled with the challenge of accurately defining illegal content while ensuring that freedom of expression is not unduly curtailed. This challenge is mirrored in the DSA by the numerous provisions that include remedies for users whose content has been removed or whose accounts have been blocked.[114]

---

[111] ibid 47.
[112] Daphne Keller, 'The European Union's New DSA and the Rest of the World' in Joris van Hoboken and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023) 236.
[113] Barata and others (n 13) 23-24.
[114] Manganelli and Nicita (n 4) 192-93.

Additionally, Article 34 adopts a distinct stance on illegal content: the term is not employed to denote specific information necessitating targeted action by platforms, as seen with notice-and-action mechanisms, but rather to characterise illegal content as not just a wide-ranging category but also as a collective issue to be evaluated by Very Large Online Platforms (VLOPs) in entirety. The phrasing of the article appears to merge these methodologies, indicating that platforms might have to devise content moderation policies aimed directly at users, accounts, pages, etc., that have been or could reasonably become origins of illegal content. Moreover, there is an absence of any suggestion of implementing potential – and obligatory – protections to mitigate any undue and disproportionate effects on the right to freedom of expression for users and third parties, whether by the platforms themselves or by regulatory authorities.[115]

6.2. Content moderation rules

The DSA intersperses content moderation rules throughout its text, yet this dispersion aligns with the proposal's rationale, which is to implement asymmetrical regulations contingent on the category of intermediary in question. On a substantive level, the DSA introduces, for the initial time in EU legislation, obligations for transparency and due diligence concerning content moderation practices; standardised notice and action protocols, necessitating justifications for content removals; and rules on account suspensions, providing users with the capacity to contest decisions on content moderation.[116] Very Large Online Platforms (VLOPs) must adhere to supplementary regulations to facilitate extensive public scrutiny of their content moderation practices. Service providers are obliged to unambiguously articulate in their terms and conditions any restrictions applied to users and maintain transparency regarding the processes

[115] Barata and others (n 13) 18.
[116] ibid 35.

and circumstances under which illegal content, or content that violates their terms and conditions, might be removed or disabled.

Intermediary service providers would need to implement notice-and-action systems to allow individuals and organisations to report potentially illegal content. The DSA specifies the details that must be included in such notices. Should a notice comprise all required elements, the provider is considered to have actual knowledge, potentially incurring liability for the illegal content of third parties if it is not removed. Upon receiving a notice, the provider must swiftly acknowledge receipt (noting whether any automated processes were utilised) and communicate their decision to the notifier. This decision must be made promptly, fairly, and impartially, and the notifier must be informed of any available remedies. Providers choosing to take down or restrict content must inform the affected user of this action concurrently with the removal, providing a clear rationale that should cover aspects like the evidence leading to the decision, any use of automated tools, and reference to the legal grounds or breach of the provider's terms and conditions. These decisions and justifications should be recorded in a public database maintained by the European Commission.

Article 7 of the DSA clarifies that intermediaries do not forfeit their exemption from liability simply by conducting voluntary, proactive investigations or other measures to identify and deal with illegal content or to fulfil the obligations of Union law, including those stipulated in this Regulation. Recital 22 of the DSA notes that providers can gain actual knowledge or awareness via such proactive investigations or through sufficiently detailed and substantiated notices according to the Regulation. Recital 26 reaffirms this concept, stating that carrying out such investigations does not disqualify service providers from liability exemptions provided by this Regulation, as long as the investigations are conducted in good faith and diligently.

Proactive investigations are shielded by immunity when they are directed 'solely' towards two primary goals: addressing illegal content or fulfilling additional obligations that intermediaries may have under the DSA and other pertinent EU laws. Regardless of whether providers may claim an exemption from liability on a case-by-case basis and despite the fact that they cannot be subjected to any general monitoring duties, the DSA introduces a range of general 'duties of care' that apply to (all) providers of intermediary services, adding a new dimension of responsibility.

The question arises in particular in connection with the exemption from liability for hosting services, which is currently contained in Article 14 ECD and Article 6 DSA. The CJEU has ruled quite extensively on this issue, notably in Google France[117], L'Oréal v eBay[118] and YouTube[119] (note that the latter judgement dates from after the adoption of the DSA proposal).[120]

Beyond the stipulations of Article 6, Article 16 of the DSA details the criteria for notice-and-action mechanisms that can engender such knowledge or awareness. Article 16(2) requires notices to include 'an explanation of the reasons why the individual or entity considers the information in question to be illegal content'. Within this framework, Article 16(3) confirms that notices providing such an explanation 'shall be considered to give rise to actual knowledge or awareness'. Nonetheless, it is crucial to emphasise that a user's assertion that content is illegal does not automatically constitute knowledge or awareness as per Article 6, unless the reported content exhibits a certain level of clear illegality.[121] Similarly, Recital 22 of the DSA

[117] *Google France SARL and Google Inc. v Louis Vuitton Malletier SA*, paras 112-114.
[118] Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others* [2011] ECR I-06011, paras 112-113.
[119] Joined Cases C-682/18 and C-683/18 *Frank Peterson v Google LLC and Others and Elsevier Inc. v Cyando AG* [2021] EU:C:2021:503, paras 105-106.
[120] Wilman (n 96) 39-40.
[121] Barata and others (n 13) 13-14.

states that notices need to be 'sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and where appropriate act against the allegedly illegal content'. According to Recital 22, the removal or blocking of access 'should be undertaken in the observance of the principle of freedom of expression'.

Under the DSA, complaints submitted by trusted flaggers – entities that can be recognised under certain conditions by Member States – must be given precedence in complaint-handling processes (Article 22). Article 22 requires platforms to establish expedited mechanisms for the processing of reports submitted by trusted flaggers. Trusted flaggers must be recognised as such by the DSC of the Member State concerned. The Commission will publish a register of recognised trusted flaggers. In addition, the article sets out procedures for dealing with trusted flaggers who submit unfounded or incorrect notices. The enhanced prerogatives of the trusted flaggers are also accompanied by greater responsibility and the Committee of Ministers of the Council of Europe warns in its 2021 content moderation guide against relying too much on trusted flaggers.[122] There is a fear that entities will be created that would monopolise the concept of scientific truth at the expense of democratic debate.[123]

There are also provisions in place to safeguard against the misuse of the complaint systems, preventing the unwarranted flagging of lawful content, applicable not just to trusted flaggers but to the entire complaints system (Article 23). Furthermore, for online platforms, there is a duty to notify the relevant law enforcement authorities if they come across information suggestive of serious criminal offences that pose a threat to people's lives or safety (Article 18). There is also a requirement for platforms to collect, endeavour to verify the credibility of,

[122] Steering Committee for Media and Information Society, *Content Moderation, Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation* (2021).
[123] Jougleux (n 29) 203.

and disclose particular information about merchants utilising the platform's services for distance contracts with consumers (Article 30).

The DSA Regulation introduces a so-called good Samaritan clause. However, it has been argued that this clause could lead to excessive removal of content as, unlike under the US Safe Harbour and US Good Samaritan clause, providers are not guaranteed protection if they fail to remove content after discovering illegal content themselves. To be sure that they cannot be held liable for illegal third-party content, providers may prefer to remove or block access to the potentially illegal content, which could lead to excessive deletions that could undermine the protection of fundamental rights and, in particular, freedom of expression.[124]

6.3. Challenging content moderation decisions

Online platforms would be required to provide their users with a means to contest decisions on content moderation. Initially, this would involve establishing internal systems for handling complaints about such decisions. These complaints must be kept on record for a minimum of six months following the decision in question. The systems should be electronically accessible, free to use, and straightforward to navigate. Complaints must be processed quickly, carefully, and impartially, and there should be the potential for a decision to be overturned without unreasonable delay. Platforms are also obliged to inform the complainants of the outcome of their complaint and the options for further recourse in a timely manner.

These regulations aim to guarantee that users are provided with sufficient means to contest any platform actions that negatively impact them, as noted in Recital 58. This pertains to content removal as well as the restriction or termination of user accounts. The procedures necessitate the reversal of decisions if the unlawfulness of the content is unverified or if there has been no

[124] Barata and others (n 13) 35-36.

breach of the platform's terms of use. Users should be informed of the outcomes of their complaints and the availability of alternative dispute resolution methods. Importantly, decisions should not rely solely on automated processing.

The fundamental principle of the DSA is to ensure that any person whose rights have been impinged upon has access to legal recourse to rectify the situation. This notion, that any breach of rights should be remediable, is encapsulated in Article 17 of the DSA. This Article stipulates that any content restriction by a hosting service provider should be paired with a detailed explanation to the service's affected recipients. The explanation must also encompass details on the remedies available, such as internal complaint resolution procedures (Article 20), alternative dispute resolution methods (Article 21), and the option for judicial recourse. Thus, the DSA presents three distinct avenues for redress that can be pursued either successively or independently. Judicial recourse is not specified within its own clause in the DSA, as it falls under the jurisdiction of national laws and procedures. Nonetheless, the DSA consistently affirms the necessity of this pathway being accessible.[125]

Article 17 mandates that platforms providing content moderation actions, which include but are not limited to content removal or account suspension, as well as actions like de-ranking or demonetisation, must supply affected users with a rationale for these actions. Notably, the DSA does not stipulate the need for such a rationale when a platform opts not to enact moderation actions in response to a notice. Despite the provision's somewhat limited remit, Article 17 significantly enhances transparency by obligating platforms to detail the extent and nature of the action taken (thereby clarifying instances of 'shadow banning') and the legal or contractual basis for the measure.[126] Under Article 20, the DSA instructs platforms to develop internal

[125] Kuczerawy (n 62) 169-70.
[126] Pietro Ortolani, 'If You Build it, They Will Come: The DSA 'Procedure Before Substance' Approach' in Joris van Hoboken and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023) 156-57.

systems for handling complaints, drawing inspiration from the Platform-to-Business Regulation. This article highlights that the notification system should be accessible not just to the directly impacted users but also to third parties who, although not platform users themselves, may wish to file a notice (such as concerning a user's post). Moreover, this system should also cover decisions pertaining to the assessment or dismissal of notifications (like the removal or blocking of content or reinstating it online). A critical aspect of Article 20 is the requirement for platforms to overturn their previous content moderation decisions (that is, to acknowledge the notice or disregard it) if the complaint presents adequate justification for such a reversal.[127]

Of course, the platforms' decisions do not restrict users' ability to seek redress in court: content moderation is not, after all, a form of arbitration. However, because the platforms control the infrastructure that enables the independent enforcement[128] of their own decisions, content moderation procedures are ultimately the main route through which a large number of parties seek redress. The outcome of these proceedings is often not reviewed by a state court.

In practise, the lack of detail in Article 20 may prove detrimental to the ability of internal complaints procedures to ensure effective access to justice: experience with international arbitration, for example, shows that the success of an alternative dispute resolution mechanism depends (among other factors) on the availability of a predictable procedure that remains comparable across different service providers.[129]

[127] Kuczerawy (n 62) 173.
[128] Pietro Ortolani, 'The Three Challenges of Stateless Justice' (2016) 7 Journal of International Dispute Settlement 596.
[129] ibid.

6.4. Out-of-court dispute settlement

Users impacted by a content moderation action should have the option to resort to an accredited out-of-court dispute resolution mechanism. The DSA delineates the criteria for the Digital Services Coordinator to certify such dispute resolution bodies. Article 21 DSA allows the Digital Services Coordinators of each Member State to certify the dispute resolution bodies established on their territory, following a procedure that only partially corresponds to Article 20 of the Alternative Dispute Resolution Directive (ADR)[130]. These rules are designed specifically to ensure that the entities operate impartially and independently from the online platforms, possessing the requisite expertise. The platforms are expected to engage with the chosen dispute resolution body in good faith and are obligated to adhere to the resolution. Should the dispute be resolved in the user's favour, the platform is required to cover all fees and costs the user has incurred due to the decision. Similarly, the European lawmakers have already tried to meet consumers' need for dispute resolution by promoting alternative dispute resolution through the and the Online Dispute Resolution Regulation.[131]

Platforms are required to notify users about the option to utilise a dispute resolution body and must generally engage in the procedure with genuine intent. However, they are not compelled to abide by the result of the procedure (Articles 21-23). Nonetheless, this does not render out-of-court dispute resolution processes ineffectual. The cost associated with these procedures remains significantly more appealing to users in comparison to litigation, and under Article 24 concerning transparency, platforms must report 'the proportion of disputes in which the online platform provider has implemented the body's decision'. Furthermore, adhering to the

[130] Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC [2013] OJ L165/63.
[131] Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) [2013] OJ L165/1.

outcomes of these out-of-court resolutions may form part of the risk mitigation strategies for Very Large Online Platforms (VLOPs) as per Article 35.[132]

Recipients of services also have the right to lodge a complaint against the provider (if the provider is in breach of the DSA) with the Digital Services Coordinator (DSC) of the Member State in which the recipient resides. However, this is not a dispute resolution mechanism, as the DSC only has to assess the complaint and, if necessary, forward it to the DSC of the establishment.[133] Besides the option to submit a complaint to the relevant DSC (Article 53), pursuing legal action remains an alternative under the DSA. The various dispute resolution methods detailed do not hinder the right of individuals to seek legal redress, for instance, to demand the removal or reinstatement of online content. Additionally, Article 54 explicitly safeguards the right of consumers to seek compensation for breaches of the DSA.

Despite the fact that legal disputes involving very large platforms are usually cross-border, the DSA does not contain any specific jurisdiction rules, meaning that plaintiffs must rely on the Brussels I bis Regulation[134] to establish the jurisdiction of a court in an EU Member State. This could prove difficult in practise: For example, some claimants might not qualify as consumers[135] and thus not be able to establish the jurisdiction of their home court.[136]

A final level of doubt concerns the possible role of collective redress: could class actions become a tool to protect marginalised or vulnerable groups affected by harmful online content? From this point of view, the DSA introduces some important innovations. Firstly, Article 90

[132] Ortolani, 'If You Build it, They Will Come: The DSA 'Procedure Before Substance' Approach' (n 126) 159-60.
[133] Barata and others (n 13) 37-38.
[134] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2012] OJ L351/1.
[135] Case C-498/16 *Maximilian Schrems v Facebook Ireland Limited* [2018] EU:C:2018:37.
[136] Ortolani, 'If You Build it, They Will Come: The DSA 'Procedure Before Substance' Approach' (n 126) 160-61.

amends Annex I of the Collective Redress Directive[137], extending the possibility already existing in some Member States, of class actions in content moderation disputes. In addition, Article 86 allows recipients of intermediary services to authorise a representative body to exercise their rights on their behalf.[138]

6.5. Rules on advertising

The data held by major technology firms is utilised not only to draw in new consumers but also to deliver their services to business partners via advertising offerings. The capacity to profile the message's recipients and customise content to meet the actual or anticipated needs and preferences of consumers results in certain materials, including adverts, being directed at a selective audience. Consequently, advertising revenue stands as a key measure of a company's stature within the digital marketplace. Over the past half-decade, there has been a significant shift in the landscape of the world's preeminent tech corporations, characterised by the reinforcement of the largest entities, the rapid rise of new entrants, and a flurry of mergers and acquisitions.[139] According to Ambroziak:

> In 2020, the 25 largest media companies accounted for 67% of all industry advertising revenues, while five years earlier the same companies accounted for only 42%. As far as the biggest players are concerned, in 2020 the share of the top ten global media owners in advertising revenues reached 55.2%, of which almost 62% belonged to Google and Facebook.[140]

---

[137] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L409/1.
[138] Ortolani, 'If You Build it, They Will Come: The DSA 'Procedure Before Substance' Approach' (n 126) 161-62.
[139] Ambroziak (n 7) 14.
[140] ibid 14-15.

In application, the DSA mandates that 'online platforms' must transparently declare when an advertisement is shown, who has financed the advert, and provide 'meaningful information' on why the advert was presented to a specific individual (Article 26). The details to be disclosed include the content of the advertisement, the identity of the natural or legal person sponsoring the advert, and whether the advert was explicitly directed at one or more distinct groups of service recipients, and if so, the principal parameters used for this targeting. This regulation overtly deems covert marketing practices illegal. By leaving the term 'meaningful information' (Article 26) subject to interpretation and entrusting platforms with the discretion to decide the granularity of the advertising data made public (such as breakdown by age group, gender, etc.), the DSA permits companies to reveal only as much non-sensitive information as their business models accommodate.[141] The DSA also bans the use of sensitive data categories as defined by the General Data Protection Regulation for creating advertising profiles. Moreover, it is prohibited to utilise data from individuals identified as minors for advertising purposes.

Furthermore, the regulation requires VLOPs to make available advertising transparency data via application programming interfaces (Article 39), even a year following the campaign's conclusion, in a manner that permits large-scale systematic analysis of the data.

The Commission is set to support and promote the formulation and application of voluntary codes of conduct for online advertising (Article 46) by online platforms and various entities. However, there is a concern that such codes of conduct may serve as a token gesture for both platforms and regulatory bodies, suggesting the presence of legal governance in digital realms while lacking real significance.[142]

---

[141] Nayanatara Ranganathan, 'Regulating Influence, Timidly' in Joris van Hoboken and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023) 207.
[142] ibid 203.

7. Platform-specific rules in the DSA

The Digital Services Act (DSA) establishes a variety of intermediary service provider categories to tailor the new rules to each category based on their significance. Yet, the fundamental differentiation among these providers, as outlined in the e-Commerce Directive (ECD) for determining the scope of liability exemptions, is preserved. While transitioning to a regulation may harmonize the varied national interpretations or implementations of these provider categories, ambiguities might persist due to the insufficient elucidation of terms like mere conduits, caching, and hosting services. Additionally, no further distinctions are introduced, despite Recital 28's intention to acknowledge that newly emerged services might fit into existing classifications. Nonetheless, it is a significant development that online platforms are now recognized as a distinct, more precisely defined group of hosting services, which can have particular responsibilities assigned to them. The current hesitance to refine the concept of platform 'neutrality' and the continued reliance on the active versus passive host dichotomy will probably result in ongoing interpretative challenges and ought to be revisited during the legislative process. The DSA does take into account the size of platforms as a pertinent factor in deciding the scope of their duties, though it is still under debate which obligations should be universally applicable.[143]

7.1. Hosting services

Every hosting provider is required to set up notice-and-action mechanisms that facilitate the simple electronic submission of reports on unlawful content (Article 16). For a report to constitute 'actual notice', it must adhere to a standardised format and include: a) the notifier's rationale for deeming the content unlawful; b) the precise URL(s) where the contentious

[143] Cole, Etteldorf and Ullrich (n 1) 38.

content is located; c) the notifier's name and email address; d) a genuine declaration confirming the veracity of the information provided. The provider is obliged to promptly acknowledge receipt of the report to the notifier and to communicate once a decision is reached. Should an automated system render the decision, this detail must be included in the notification. Decisions must be made without undue delay.

Furthermore, any action taken to remove content, whether in response to a notice or through proactive steps, must be reported to the service user who posted the content (Article 17). This notification should minimally consist of: a) the rationale behind the removal; b) the geographical scope of the removal; c) an indication of whether the decision was made through automated processes; d) the legal foundation if the content is indeed illegal; e) a citation of the pertinent contractual clauses if the content breaches the terms of service; and f) the legal avenues available for contesting the decision. Moreover, all decisions to remove content, along with their justifications, must be recorded in a publicly accessible database maintained by the European Commission.

7.2. Online marketplaces

Article 30 mandates specific prerequisites for online marketplaces concerning the traceability of traders. These obligations, akin to 'Know Your Customer' (KYC) norms, necessitate gathering information such as addresses and bank details, verification of identity, commercial register identifiers if relevant, and a declaration from the traders affirming that their goods adhere to EU regulations. This information is required to be validated for authenticity with a reasonable level of diligence. Should the information prove to be incomplete or unverifiable, the platform must cease its commercial engagement with the trader.

Additionally, online platforms are required to structure their online interfaces to enable traders to comply with all other obligations derived from pre-contractual disclosure and product safety

information as per EU legislation. This provision applies exclusively to intermediaries that function as marketplaces. Platforms are expected not just to identify repeat infringers but also to vet traders (sellers) prior to establishing a commercial relationship. The rationale for these extended duties is twofold: the significant influence of e-commerce on the internal market, especially the free movement of goods, and the pre-existing due diligence mandates in adjacent realms of EU consumer law and anti-money laundering regulations.[144] The infringements targeted by this article are intellectual property rights and consumer and product safety laws (Recital 72). This important passage is a welcome and much-needed tool for product and food law enforcement authorities to incentivise platforms to act as responsible actors when they offer sellers the possibility to list products that pose particular safety risks and for which mandatory online information requirements exist.[145]

Given the risks to users' rights and fundamental values by the dissemination of illegal content and the difficulties associated with enforcement action against users when their identity cannot be verified, consideration should be given to extending elements of a KYC approach in a similar way to content dissemination platforms. Platforms would then potentially have to be considered responsible for the content disseminated (or be sanctioned under the new regime) if they do not take measures to identify users (or refuse to provide information about their 'customers' when requested by a court).[146]

---

[144] 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 [2005] OJ L149/22; Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L141/73.
[145] Cole, Etteldorf and Ullrich (n 1) 198.
[146] ibid 199.

7.3. Start-up companies and SMEs

Article 19 exempts micro and small enterprises from due diligence responsibilities concerning complaints and redress mechanisms, trusted flaggers, the misuse of their services, out-of-court settlements, serious criminal offences, the traceability of traders, reporting transparency, and the transparency of advertising – as stipulated in Articles 20 to 28, except when they qualify as a very large online platform (as per Recital 57).

The mandate for all providers to designate Single Points of Contact (SPoCs) or legal representatives (Articles 11, 12, and 13), and for clear terms (Article 14) concerning content restrictions and the use of algorithmic systems, is justified, including for micro and small enterprises. This will compel all firms, including startups, to clarify to their customers and themselves from the outset their values, principles, and methods related to responsible conduct. Concurrently, it is deemed suitable to relieve micro and small enterprises from the obligation of transparency reporting.

7.4. Internet service providers

The requirement for all intermediaries, encompassing internet access providers (and caching services), to issue transparency reports on their content removal practices is also seen as fitting. Internet Service Providers (ISPs) have concerns regarding the spread of automatic takedown and filtering systems as well as dynamic injunctions, and providing information on these matters would enhance the overall understanding. Given their critical role in infrastructure, their inclusion in the obligation for cross-border reporting is to be commended. This obligation would also yield insights into the role of internet registrars/registries in combating illegal content if they are classified as one of the intermediary service categories.[147]

[147] ibid 196.

In an age where virtual private networks (VPNs) and proxy servers are commonplace, the absolute effectiveness of content filtering measures may be questionable. However, the approach outlined suggests that 'effectiveness' should be interpreted as creating obstacles that complicate the achievement of unlawful aims, thereby actively discouraging users from attempting to access the unlawful content through the services of the targeted provider. The goal is not to create an impenetrable barrier to access, but to raise sufficient barriers to dissuade attempts to access the content.[148]

7.5. Online platforms

Online platforms are obliged to enhance their transparency reporting, in addition to the broad duties imposed on all intermediaries as per Article 24. These supplementary mandates include disclosures about alternative dispute resolution processes and their results, the frequency of account suspensions resulting from illegal content notifications, instances of wrongful notification submissions, and baseless objections, along with metrics regarding the implementation of automated content moderation. This includes its intent, decision-making accuracy, and the protective measures enforced. Furthermore, these platforms are required to disclose data on their average monthly active users within each EU Member State biannually. The Commission has the prerogative to prescribe uniform templates for such reports. Article 26 mandates that digital platforms must transparently communicate with users about the advertisements, identifying the advertiser and outlining the parameters used for presenting advertisements to users.

[148] Jougleux (n 29) 179.

When compared with another EU regulation for the digital domain that is currently being discussed, specifically the AI Act[149], the DSA has chosen to use a criterion based on size instead of a precise risk-based model (namely, the high-risk threshold proposed in the AI Act). This is because, in a context where network effects are central, the size of a platform acts as a surrogate for the level of risk, which does not automatically apply in other sectors – such as AI – where there is potential for diverse applications.[150] Regarding the structure of the DSA, Articles 34, 35, and 37 are the key sections concerning risk management: Article 34 pertains to assessment, Article 35 to risk mitigation, and Article 37 to the supplementary role of independent audits.

7.6. Very large online platforms

Very large online platforms (VLOPs) as defined in Article 33 of the DSA, i.e., those that provide their services to a number of average monthly active recipients of the service in the Union of 45 million or more, to be calculated in accordance with the methodology to be set out in delegated acts of the Commission, will have to assume new obligations under the DSA to assess and mitigate 'systemic risks'. The existence and nature of these risks are not clearly described or demonstrated by the legislator. Recital 79 states that the way platforms design their services is 'generally optimised to benefit their own advertising-driven business models and can cause societal concerns'. Article 34(1)(b) describes systemic risks related to fundamental rights as:

> [A]ny actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter (CFREU), to respect for private and family life enshrined in Article 7 of the Charter, to

[149] Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislactive acts' COM (2021) 206 final.
[150] Alessandro Mantelero, 'Fundamental Rights Impact Assessment in the DSA' in Joris van Hoboken and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023) 110.

> the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter.[151]

VLOPs are at least once a year required to carry out assessments of systemic risks taking into account the extent to which the various systems (e.g. content moderation, recommendation systems, advertising tools) set up on their platform pose risks (Article 34). The DSA imposes due diligence obligations on VLOPs to identify, analyse, assess and mitigate some categories of systemic risk: (i) illegal content, (ii) actual or foreseeable negative impacts on the exercise of fundamental rights protected by the Charter, (iii) actual or foreseeable negative impacts on civil society discourse and electoral processes and on public security, and (iv) actual or foreseeable negative impacts related to gender-based violence, the protection of public health and minors, and serious negative consequences for the physical and mental well-being of the person concerned (Articles 34 and 35). Risk assessment is useful in two ways: firstly, it serves as a tool of transparency in relation to the moderation policy, and secondly, it is a prerequisite for the fundamental new risk management obligation in Article 35.[152]

In other words, DSA introduces a 'due diligence' obligation of care to mitigate risk, requiring online platforms to operate a moderation service independently of the notification system. This moderation works on the basis of the specific risks. This duty does not mean that online platform is not automatically liable for illegal content on the platform. Online platform's immunity from secondary liability for the publication of illegal content remains in place. In

[151] Digital Services Act, art 34.
[152] Jougleux (n 29) 181.

addition, there is primary liability if it is proven that online platform does not exercise a reasonable degree of diligence in managing the platform with regard to compliance with the rule of law. Prior to that, however, online platforms would be obliged to carry out an independent audit of compliance at regular intervals. Regardless of the changes, clarifications and additions to the existing safe harbour mechanisms, the DSA follows a clear path established by the General Data Protection Regulation (GDPR)[153] to impose controls on the private sector in relation to citizens' fundamental rights. The GDPR supervisory authority becomes the 'Digital Services Coordinator' (a European board for Digital Services is also established), the Data Protection Officer becomes the 'Compliance Officer', and the Data Protection Impact Assessment becomes the 'Risk Assessment'. It should be mentioned that the Digital Services Coordinator is empowered under Article 52 to impose fines for non-compliance with this Regulation.

Such compliance measures may include, where applicable: a) adapting content moderation or recommendation systems, their decision-making processes, the characteristics or functioning of their services or their terms and conditions; b) targeted measures to limit the display of advertisements in connection with the service they offer; c) strengthening internal procedures or monitoring of their activities, in particular with regard to the detection of systemic risk; d) initiating or adapting cooperation with trusted flaggers in accordance with Article 22; e) initiating or adapting cooperation with other online platforms under the codes of conduct and crisis protocols referred to in Articles 45 and 48 respectively.[154]

In the case of VLOPs, the DSA's meta-regulatory essence is particularly evident: once identified, these entities are effectively required to function as risk regulators, under the

[153] ibid 181.
[154] ibid.

surveillance and governance of the European Commission, the National Digital Services Coordinators, and the European Board for Digital Services, acting as meta-regulators. Specifically, Article 34 obliges VLOPs and VLOSEs to conduct routine evaluations of any systemic risks stemming from the design or functioning of their service and related systems (including algorithmic systems), or from the utilisation of their services, and to furnish information to the Commission and the Digital Services Coordinator when requested. Furthermore, Article 35 stipulates that they must implement suitable, proportionate, and effective actions to mitigate such risks. A comparable mandate was introduced rather late in the DSA deliberations (in 2022, subsequent to Russia's invasion of Ukraine) for a 'crisis' scenario, that is, exceptional circumstances that result in a severe threat to public safety or health in the EU or a significant part thereof.[155] Per Article 36, in such a scenario, the Commission may instruct VLOPs and VLOSEs to evaluate and mitigate the risks of their contribution to the serious threats identified and to provide regular reports on the same. To demonstrate adherence to the aforementioned requirements, VLOPs and VLOSEs are compelled to undergo independent audits at their own cost and at minimum annually as per Article 37 to ascertain compliance.

The DSA mandates that very large online platforms (VLOPs) submit to external and independent audits performed by accredited and impartial auditors (Article 37) and, following a negative audit outcome, to heed any operational suggestions made by the auditors by formulating an audit implementation report within one month. Specific duties are further introduced for instances in which VLOPs employ recommendation systems (Article 38) or present online advertisements on their platforms (Article 39).

[155] Nicolo Zingales, 'The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence: Hail To Meta-Regulation' in Joris van Hoboken and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023) 215-16.

Article 38 imposes extra conditions for the transparency of recommendation algorithms. VLOPs are to furnish straightforward information in their terms of service about the factors influencing their recommendation algorithms and the methods for users to modify these factors, along with providing users the facility to make these adjustments through readily accessible functions. Article 39 mandates further requirements concerning the transparency of advertising. Under this, VLOPs are required to maintain a publicly accessible database of the advertisements they display. This archive should include the content of the ads, the identity of the advertiser, the timeframe during which the ads are displayed, the criteria used for targeting the ads, and the reach and demographic data of the recipients.

The regulatory framework established for very large online platforms stipulates additional responsibilities that closely resemble those set out by the GDPR. VLOPs are obliged to facilitate access to data that is critical to monitoring and evaluating compliance within a designated timeframe (Article 40) and to designate one or several compliance officers charged with overseeing adherence to the DSA. These officers also act as a channel for collaboration with the regulatory authority (Article 41); furthermore, they are beholden to specific, heightened transparency reporting duties (Article 42). In regard to these duties, the requirement for transparency is temporally more restricted (reports are due every six months) compared to the reporting requirements for intermediary services (Article 15) and online platforms (Article 24). The scope of these reports is broadened to include the outcomes of risk assessments and the risk mitigation strategies that have been identified and put into practice (Articles 34 and 35), as well as details on the audit and subsequent audit implementation report (Article 37).

Article 40 provides options for vetted researchers to have access to VLOPs' data in order to verify platforms' compliance with the act. As a means of standardising data access, application programming interfaces – APIs are already used by social media platforms, more or less in

accordance with Article 40(7) DSA. Recently, YouTube opened its API to researchers.[156] Article 44 DSA on standards states that APIs could also be developed as voluntary standards for the transmission of notices by trusted flaggers as well as for advertising repositories (Article 39 DSA), with the support of the European Commission and the European Digital Services Board.[157] VLOPs must designate compliance officers as per Article 41, who are tasked with overseeing the platform's compliance with the DSA. These officers are expected to possess the necessary qualifications and experience to fulfil their responsibilities. Their primary functions include engaging with the pertinent Digital Services Coordinator (DSC), supervising the platform's execution of the independent audit, providing advice to management and staff on compliance matters, and monitoring the VLOP's adherence to the regulations.

VLOPs must submit a transparency report every six months (Article 42). In addition, they must submit a report on the conduct of the annual audit, addressing the issues identified in it. If VLOPs have concerns about disclosing confidential information and information that would pose other security risks, they can provide this information in a full report only to the relevant DSC and delete this part of the information for the public report.

The Commission endorses and promotes the formation, enactment, and renewal of voluntary sector standards, particularly concerning specific technical aspects of the DSA Regulation like the electronic submission of notices or the audit processes for VLOPs (Article 44). It advocates for and assists in the creation of codes of conduct at the Union level to aid the proper implementation of the Regulation (Article 45), notably in the realm of online advertising (Article 46). Codes of conduct serve as a tool to control and lessen systemic risks associated with VLOPs that impact numerous platforms. Moreover, the Commission will promote and

[156] 'YouTube Researcher Program' <https://research.youtube> accessed 10 December 2023.
[157] Catalina Goanta, 'Now What: Exploring the DSA's Enforcement Futures in Relation to Social Media Platforms and Native Advertising' in Joris van Hoboken and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023) 146.

support the involvement of VLOPs and, where suitable, other online platforms in the development, trialling, and implementation of 'crisis protocols' intended to address crisis events strictly confined to exceptional situations that threaten public security or health (Article 48). These crisis protocols, confined to 'extraordinary circumstances', are intended to establish clear procedures and responsibilities for the entities involved, safeguarding actions, and reporting mechanisms to handle such crises.

The supervisory rules outlined in Articles 49 to 60 are adjusted by Articles 64 onwards of the DSA concerning the regulation of VLOPs. Within this structure, the Commission is positioned at the core of supervisory activities. The oversight of VLOPs is not entirely shifted from the Digital Services Coordinators (DSCs) of the place of establishment to the Commission. Instead, specific procedures are envisaged with significant participation and ultimate decision-making authority vested in the Commission. This is relevant to the establishment of expertise and capabilities (Article 64) for VLOP infractions, which necessitates coordination among the Commission, the European Board for Digital Services (EBDS), and DSC before a DSC's decision is conclusively enacted. It pertains to the intervention powers afforded to the Commission by Article 65 of the DSA, under which it can respond, for instance, to what it deems as inadequate measures by a competent DSC.[158]

8. Enforcement of new rules across the single market

The pertinent details regarding the design and framework of oversight are principally outlined in Chapter IV of the DSA, though previous chapters also incorporate vital components as part of the overall enforcement mechanism, particularly in terms of information and data gathering.

[158] Cole, Etteldorf and Ullrich (n 1) 112.

The DSA establishes multiple tiers of cooperation mechanisms that interlink the various levels of supervision (national supervisors, Digital Services Coordinators, and the Commission), with the principal platform for this being the European Board for Digital Services (EBDS). This consultative body, consisting of the Digital Services Coordinators and led by the Commission, is designed to foster a collective Union perspective on the consistent implementation of the Regulation and collaboration at an international level on suitable investigative and enforcement actions. This is particularly achieved through the creation of templates and codes of conduct, as well as the scrutiny of emerging general patterns in the evolution of digital services within the Union. Furthermore, the DSA encompasses a range of cooperation mechanisms within many of its provisions concerning specific investigations, procedures, and decisions that connect Digital Services Coordinators amongst themselves and with the Commission. In this context, the sharing of information is vital, which is the rationale behind Article 85 that mandates the establishment and maintenance of an information exchange system by the Commission.[159]

The DSA establishes specific mechanisms and presents multiple challenges for the devolution of supervision to the Member State level. For instance, the introduction of Digital Services Coordinators (DSCs) is mandated, which are to be endowed with independent regulatory powers at the national level. The foundational standards for these powers are specified within Article 51. These DSCs are pivotal to supervisory actions and function both as facilitators amongst various national regulatory bodies and as contributors at the international level within the newly formed European Board for Digital Services (EBDS). They also act as liaisons for DSCs in other Member States and the European Commission.[160]

---

[159] Elżbieta Kawecka-Wyrzykowska, 'Proposal for an EU Digital Levy: Challenges and Possible Implications' in Lukasz Dawid Dąbrowski and Magdalena Suska (eds), *The European Union Digital Single Market: Europe's Digital Transformation* (Taylor & Francis Group 2022) 113.
[160] Cole, Etteldorf and Ullrich (n 1) 111-12.

Article 49(1) of the DSA stipulates that Member States must appoint one or more authorities competent for the implementation and enforcement of its rules. Article 56 outlines the competences aligned with the creation of national supervisory bodies: A service provider is to fall under the jurisdiction of the Member State in which it has its main establishment, or if lacking an establishment within the Union, where its legal representative is resident or established – the appointment of a legal representative being obligatory for all intermediary services based outside the EU, as per Article 13 of the DSA. Yet, Article 56 does not delineate specific criteria for determining the place of establishment as the AVMSD does.[161] Instead, such definitions are provided in Recital 76 of the DSA, which refers to the main establishment or head office and imposes the condition that significant financial activities and operational oversight occur at that location. For entities without an establishment, as previously noted, jurisdiction is triggered by the domicile of the legal representative, and, besides the statutory requirement, the incentive to nominate such a representative is to avoid the scenario outlined in Article 56(7) of the DSA, which states that, in its absence, jurisdiction defaults to all Member States. For the latter situation, the only introduced limitation is that Member States must notify others if actions are taken based on this competency allocation and ensure that no concurrent actions are taken that would contravene the *ne bis in idem* principle. In addition, Article 49(2) requires one of the competent authorities to be designated as the DSC, which acts as the central contact point and coordinates the cooperation of the various supervisory authorities at national level if several supervisory authorities are involved.[162] The provision as part of EU law does not detail the operational framework of such coordination at the national level. Alternatively, the DSC could be envisaged as the sole authority charged with enforcing the DSA within a

[161] Art 2 para 3 defines, relying on a graded layer of criteria such as the question where programme-related decisions are made, where for the purposes of the AVMSD a media service provider shall be deemed to be established in a Member State.
[162] Barata and others (n 13) 39.

Member State. In either model, the DSC bears the responsibility of facilitating cooperation with other DSCs, the committee established under the DSA (European Board for Digital Services), and the Commission at the international level.[163]

8.1. Country of origin principle

The 'Country of Origin' (COO) principle is a fundamental component of the internal market; thus, it serves as a foundational aspect of the Electronic Commerce Directive (ECD). Article 3(1) of the ECD mandates that Member States must ensure that Information Society Services (ISS) established within their jurisdiction, the COO, adhere to the domestic regulations of that Member State when they operate across the EU. In turn, the principle of the internal market prevents Member States from imposing restrictions on the freedom to provide services of ISSs based in another Member State, under the laws of their own (destination) country. Consequently, ISS are generally required to comply with the legislation of only one Member State and are free, in principle, to offer their services in other Member States. This approach was considered valid when the ECD was formulated, as the EU aimed to foster legal certainty with certain rules within a harmonised regulatory framework for the then-emerging e-commerce services, whilst guarding against the potential negative effects of jurisdictional arbitrage and rule fragmentation. The COO principle is confined to the EU internal market, given that the ECD lacks extraterritorial reach. This implies that content from ISS outside the EU targeting EU consumers does not come under the directive's purview and hence can be dealt with by individual Member States according to their national laws. The COO principle not only underpins the ECD but is also integral to other relevant EU legislation, especially concerning the dissemination of online content, such as the Audiovisual Media Services Directive (AVMSD). Despite some variances in the incorporation of the COO into both

[163] Cole, Etteldorf and Ullrich (n 1) 211-12.

directives, a combined examination reveals that the COO remains one of the pivotal principles of EU regulation of online content.[164]

Under Article 2 of the DSA, the regulation is applicable to intermediary services offered to users who are established or resident within the Union, regardless of the provider's location. Article 2(2) outlines the broadened territorial scope. In divergence from the ECD, the DSA also encompasses intermediary services not based in the EU, but which operate within the internal market in a manner that indicates a substantial connection with the EU (as mentioned in Recital 7). This extension makes the regulation's reach extraterritorial, in that the participation in the market is key, not the provider's physical location, meaning that EU regulations are also imposed on companies from third countries. This approach mirrors that of the General Data Protection Regulation – specifically Article 3(2). Recital 8 draws on the established methodology and targeting criteria from the Brussels I Regulation and the principles of private international law, as well as the ECJ's jurisprudence, to ascertain the existence of a substantial EU connection.[165] Article 3(d) clarifies what constitutes the offering of services, determining that it involves enabling legal or natural persons in one or more Member States to utilise the services of an ISS provider that has a significant link with the Union. Such a link is presumed if the provider operates an establishment within the Union. Should there be no such establishment, the determination of a substantial connection must be grounded on specific factual criteria, such as having a considerable number of users in one or more Member States, or targeting activities towards one or more Member States.

[164] ibid 143-44.
[165] ibid 162-63.

8.2. Specific provisions of sectoral legislation

The DSA does not interfere with the specific provisions of current and future sectoral legislation. According to Article 2, this applies to the ECD, the AVMSD, copyright and related rights, TERREG and e-Evidence Regulation and Directive, the Regulation on the marketing and use of explosives precursors, the P2B Regulation, the consumer protection and product safety acquis and the GDPR and e-Privacy Directive.

Essentially, Article 2 of the DSA decrees that its regulations do not override a variety of specific legal provisions. This can be interpreted as adopting a *lex specialis* approach in a supplementary manner. This suggests potential interactions between different legal instruments and that the DSA may provide clarifications and additional provisions for regulatory domains already covered by sector-specific measures like the DSM or the AVMSD. For instance, in the realm of illegal content mitigation, the DSA introduces concepts such as trusted flaggers or risk assessment and mitigation duties for very large online platforms. Three significant concerns have surfaced regarding the DSA's interplay with other frameworks, such as the recently enacted action plans: the cooperation among authorities on illegal online content, the comprehensive transparency of online advertising, and the promotion of European works.[166] Moreover, the DSA is expected to safeguard professionally edited broadcast content regulated at the national level, ensuring that private platforms cannot arbitrarily remove such content or 're-regulate' it based on their business models. From the perspective of creative stakeholders, there has been debate on the DSA's impact concerning the equilibrium between artistic expression freedom and the fair valorisation of intellectual property. Specifically, there are inquiries about the DSA's incremental value in the existing legal context for countering online piracy and whether the new regulations for gatekeepers will enhance the transparency of

[166] Barata and others (n 13) 119.

audience data shared between rights holders and platforms.[167] The DSA also augments the duties of traders concerning the disclosure of commercial communications, aligning with the directive on Unfair Commercial Practices.

Conversely, the DSA does not explicitly outline how complementarity will manifest in practice. From an interpretation perspective, it will be intriguing to observe the extent to which the judiciary, including the Court of Justice of the European Union, will construe the DSA in terms of its professed complementarities. Arguably even more critical is how the DSA's complementarity with other sector-specific regulations will withstand the test at the enforcement stage. The primary risk associated with the DSA's complementarity with other sectoral regulations is the emergence of ambiguities, which may result in suboptimal enforcement.[168]

8.3. Digital Services Coordinators

Article 51 outlines a detailed set of rules regarding the powers of Digital Services Coordinators (DSCs). These encompass investigative powers (the right to obtain information and to perform on-site inspections of providers and their commercial partners under certain conditions; the authority to demand explanations from any provider's employee or representative and to document their statements) and enforcement powers (the capacity to recognise and make obligatory the compliance commitments undertaken by providers); the power to order a cease of violations and apply suitable remedies when necessary; the power to impose and collect fines and/or periodic penalty payments; and the competency to implement interim measures to avert the risk of serious harm).

[167] ibid 119-20.
[168] Goanta (n 157) 141-42.

Furthermore, Article 51(3) sets out powers of last resort, which may be exercised when all previous attempts to stop a persistent breach under both this Regulation and other EU or national legislation have failed to terminate an infringement causing significant harm. These final steps involve engaging the management of the service provider to review the situation, devise and submit a detailed plan of action to conclude the breach, ensure the implementation of the necessary measures, and report on the actions taken within a specified period. In cases of serious criminal offences that pose a danger to human life or safety, DSCs are vested with the right to approach the relevant judicial authority to request a temporary limitation of access to the service for users or, if this is not feasible, to the implicated website, application, or similar platform.

Pursuant to Article 51(6), Member States must ensure that the exercise of the powers by DSCs is accompanied by suitable safeguards as established in the relevant national legislation, in alignment with the Charter of Fundamental Rights of the European Union (CFREU) and the general principles of EU law. Moreover, service recipients are entitled to file a complaint with the DSC in their home country, which is then to be sent to the DSC in the provider's country of establishment for review and, where necessary, passed on to another competent authority (Article 53). Notably, the DSA Regulation also confers authority on DSCs other than those in the country of establishment to evaluate actions taken by the competent DSC; should there be inaction or a divergent investigative outcome from the position of the enquiring DSC, the issue can be escalated to the Commission. The Commission may then call upon the establishment DSC to re-examine the matter and may ultimately substitute the DSC's powers with its own.

In terms of sanctions for intermediaries' failure to fulfil obligations as a part of the enforcement mechanism, Member States are obligated to establish rules on penalties for such violations (Article 52), which serve to reinforce the powers designated for DSCs (Article 51). These penalties must be effective, proportionate, and dissuasive, with the Regulation stipulating a

maximum limit: they shall not surpass 6% of the providers' annual income or turnover and may reach up to 1% in cases of procedural non-compliance (such as supplying erroneous or incomplete information or not amending such information), and for periodic penalty payments, 5% of the average daily turnover in the previous financial year per day.

Digital Services Coordinators (DSCs) are to act as a principal authority for receiving complaints from the public regarding breaches of regulations by intermediaries (Article 53) and are required to disclose yearly reports on their operations (Article 55). Article 57 allows for the circumstance where a DSC from one Member State or the European Board for Digital Services (EBDS) can, under certain conditions, call upon the DSC in the service provider's country of establishment to take measures if there are suspicions of DSA rule infractions, with specified deadlines in place. Should the DSCs in question disagree on the approach to be taken, the Commission will also become involved and evaluate the situation.

In addition, the DSC must also fulfil other important supervisory functions itself: it vets researchers seeking access to data on platforms (Article 40), and it can certify out-of-court dispute resolution bodies (Article 21), among other things. It must be 'completely independent' of political and economic interests (Article 50(2), Recital 111), have certain investigative and enforcement powers (Article 51) and be provided with adequate resources (Article 50(1), Recital 111). DSCs must fulfil their task in 'an impartial, transparent and timely manner' (Article 50) and they must exercise their tasks and powers 'with complete independence, (...) free from any external influence, whether direct or indirect, and [without taking] instructions from any other public authority or any private party'. In this respect, this wording is identical

to that in Article 52 of the General Data Protection Regulation on the independence of supervisory authorities.[169]

Alongside cultivating in-house proficiency, the Digital Services Coordinator (DSC) ought to develop infrastructures and nurture a culture that proactively involves and creates a network of specialists in the platform sector. One method of achieving this might be through the introduction of fellowship programmes. Companies and non-profit organisations employ a range of fellowship models from which the DSC might take cues. An alternative method for harnessing external expertise could involve establishing a DSC advisory council or round table, comprising authorities from the academic world, civic society, industry, media, and potentially users of the platforms.[170]

8.4. European Board for Digital Services

Section 3 of Chapter IV of the DSA delineates the establishment of the European Board for Digital Services (EBDS), an independent consultative collective of Digital Services Coordinators (DSCs). Its primary role is to orchestrate cooperative efforts, offer assistance and guidance, and aid DSCs and the Commission in overseeing Very Large Online Platforms (VLOPs) (Article 61). As specified in Article 62, the EBDS is to consist of representatives from the DSCs of each Member State, with these representatives being high-ranking officials. Moreover, other authoritative bodies charged with specific duties in the application and enforcement of the DSA regulations are participants in the board. Should the matters under

[169] Ilaria Buri, 'Regulator Caught Between Conflicting Policy Objectives: Reflections on the European Commission's Role as DSA Enforcer' in Joris van Hoboken and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023) 78.
[170] Julian Jaursch, 'Platform Oversight: Here is what a Strong Digital Services Coordinator Should Look Like' in Joris van Hoboken and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023) 99.

discussion be pertinent to them, additional national authorities may be summoned to board meetings.

The Commission is assigned the leadership of the EBDS, including providing administrative and analytical support; however, it does not possess the authority to vote on EBDS resolutions. The EBDS's internal procedural rules are subject to the Commission's approval.

The EBDS does not have regulatory power. Its activities are confined to providing support, coordination, and advisory services. Its general responsibilities (Article 61(2)) involve contributing to uniform and effective collaboration, coordinating and contributing to the guidelines and analyses from the Commission, the DSCs, and other authoritative entities concerning emerging issues in the internal market, and supporting the DSCs and the Commission in the supervision of VLOPs. This broad outline of duties is expanded upon in Article 63, which specifies the EBDS's roles, particularly in delivering opinions, recommendations, or advice to DSCs and fostering the creation and execution of European standards, guidelines, reports, templates, and codes of conduct. The core text of the DSA does not explicitly define how binding these actions should be or in what context they should be considered.[171] Recital 133 underscores that the regular rules apply, whereby opinions, requests, and recommendations are not legally binding, although any non-adherence to them must be distinctly justified and may serve as a barometer for the Commission to evaluate whether a Member State is fulfilling its obligations under the Regulation. Additionally, according to Article 61(1)(d), the EBDS has the capacity to prompt the Commission's intervention and commencement of proceedings as per Article 66 by requesting the Commission to take action.

[171] Cole, Etteldorf and Ullrich (n 1) 219.

8.5. Role of the European Commission

The DSA provides for a strengthened supervisory regime where VLOPs have been found by a DSC to be in breach of the provisions of Section 5 of Chapter III or has 'systematically infringed any of the provisions of the DSA in a manner that seriously affects recipients of the service'. The Commission is authorised to intervene if the infringements persist and are not sufficiently remedied by the competent DSC (Article 66). Following this intervention, the DSC of establishment shall no longer be entitled to take investigative or enforcement action in relation to the VLOP's conduct in question (Article 66), unless requested to do so by the Commission. Instead, the Commission subsequently has the relevant investigative, procedural and enforcement powers with partial involvement of the EBDS, while the involvement of the DSC is essentially limited to information rights and obligations.[172] In addition to the different layers of supervisory structures and instruments, the Commission shall be empowered to adopt delegated acts in accordance with Articles 24, 33 and 40, as further specified in Article 23.

The Commission possesses a range of tools to investigate and enforce VLOP compliance. This includes conducting inquiries via requests for information (Article 67), interviews (Article 68), and on-site inspections (Article 69). In urgent situations where there is a risk of serious harm to recipients, interim measures can be implemented (Article 70), and the Commission may formalise binding commitments proposed by VLOPs to guarantee adherence (Article 71) and oversee compliance – with the Regulation as a whole, beyond individual cases. This encompasses the right to access and require explanations concerning the databases and algorithms utilised by the platforms (Article 72). Should there be a failure to comply with the Regulation, the Commission has several powers to act against VLOPs: It can issue non-compliance decisions regarding the Regulation and levy fines for violations of the pertinent

[172] ibid 213-14.

provisions of the Regulation or of interim measures and obligations (Articles 73 and 74), including breaches of procedural regulations.

Moreover, the Commission is authorised to impose periodic penalty payments on VLOPs (and under certain circumstances, on their business partners as well). The limits for these sanctions align with those set by the DSCs, at 6%, 1%, and 5% of the applicable benchmarks, similar to Article 52. The DSA sets limitation periods of five years for the imposition (Article 77) and for the enforcement (Article 78) of penalties. To safeguard fundamental rights, Articles 79 and 80 introduce procedural protections, notably the right to a hearing and to review the case file, as well as the publication of decisions, which must consider the rights and legitimate interests of the VLOP.

The Regulation therefore endows the Commission with vast supervisory and enforcement authority over the most sizeable platforms and online search engines, particularly concerning their primary due diligence responsibilities such as systemic risk assessments, access to research data, and crisis protocols. The finalised document also mandates an annual supervisory charge that VLOPs and VLOSEs must pay to offset the costs the European Commission incurs in its supervisory duties (Article 43).

As previously noted, under the DSA, the Commission's regulatory authority extends beyond the provisions exclusively pertaining to VLOPs. This is relevant in scenarios of transnational cooperation as detailed in Article 58, wherein the Commission determines that the actions of a DSC in a cross-border case are not in alignment with the DSA. The Commission can then instruct the DSC in question to pursue the investigation and re-evaluate the situation before potentially assuming control of the case — as outlined in Article 59(3).

8.6. Audit and reporting obligations

Every VLOP is subject to independent audits on an annual basis. Furthermore, the Commission, the Digital Services Coordinators within the Member States, and accredited independent auditors are granted access to the data held by these large platforms. Civil society groups are also able to freely utilise data that is made publicly available. This provision ultimately facilitates quantitative research and ensures that access to data is not manipulated to favour researchers who may be sympathetic to the platforms while obstructing those who may scrutinise them more critically. These regulations also yield valuable insights into the behaviour of the platforms.[173]

Two articles in the DSA warrant particular attention: the obligations for audits and reporting detailed in Articles 37 and 42. Article 37 mandates that Very Large Online Platforms (VLOPs) undergo annual audits to evaluate their adherence to their duties, specifically the execution of systemic risk assessments and the implementation of corresponding mitigating actions. These audits also verify compliance with the pledges VLOPs make within codes of conduct and crisis protocols. The outcome of a negative audit carries significant consequences both for the auditing body and the VLOP. Firstly, the audit report must include 'operational recommendations on specific measures to achieve compliance'. Secondly, upon receiving such a report, VLOPs 'shall take due account of any operational measures addressed to them with a view to take the necessary measures to implement them'. Specifically, VLOPs are required – within one month of receiving the recommendations – to formulate an audit implementation report which outlines these actions or, if they choose not to follow the recommendations, they

[173] Geese (n 36) 70.

must provide their justifications for this decision and detail any alternative steps they propose to rectify the non-compliance.[174]

The audit duties outlined in Article 37 might initially serve to establish a supervisory framework that ensures VLOPs adhere to the obligations specified in the DSA. Nevertheless, delegating these audits to external private entities, which will develop their verification and reporting procedures, introduces potential hazards. The present composition of Articles 34 to 37 indicates the foundations of a prospective governance, risk, and compliance framework for online platforms that encompasses aspects of fundamental rights. This should not entail a total dependency on private audits for the oversight role, as it could erode the necessity for regulators to possess their own capacity for oversight. In essence, there is a need for them to develop the capability to scrutinise the auditors effectively. Recent instances highlight the dangers of overly relying on such audits as a substitute for direct regulatory oversight.[175] Consequently, it is advocated that this approach should be merely an initial supplementary measure leading to more direct regulatory involvement in the auditing and evaluation of online platforms' business and content management practices, which necessitates the development of the requisite expertise and capabilities.[176]

Collectively, the audit and transparency mandates stipulate external validation and supervision of VLOPs' adherence to the risk assessment and mitigation strategies. This aspect is crucial to ensure that VLOPs meet their responsibilities to detect and counter systemic risks on their platforms, which encompasses issues like disinformation, and that their efforts are evaluated,

[174] Barata and others (n 13) 55.
[175] Deirdre K. Mulligan and Kenneth A. Bamberger, 'Saving Governance-By-Design' (2018) 106 California Law Review 697 698 718-719; Julie E. Cohen, 'The Regulatory State in the Information Age' (2016) 17 Theoretical Inquiries in Law 369 403-407.
[176] Cole, Etteldorf and Ullrich (n 1) 201-02.

critiqued, and overseen independently by auditors, the Digital Services Coordinator, the Commission, and, notably, by the general public.[177]

8.7. Meta-regulatory model

The approach in the DSA, which on the one hand leaves considerable discretion to companies in the implementation of regulatory principles and on the other hand involves a process of continuous assessment and monitoring of outcomes, is referred to as 'meta-regulation'[178] or 'enforced self-regulation':[179] 'meta' because one (macro) regulator supervises another (micro) regulator in its risk management; 'enforced' because the (macro) regulator is authorised to take enforcement action if self-regulatory practises are inappropriate. To determine whether such measures are justified, the meta-regulation establishes organisational and procedural standards against which self-regulatory practises can be assessed. This gives it a fundamentally 'reflexive' character:[180] it focuses on improving the self-referential capacities of social systems and institutions outside the legal system to achieve general social goals, rather than on prescribing specific measures.[181]

The audit obligations are a crucial element for the functioning of the meta-regulatory framework, as they provide the necessary control of the implementation of the measures carried out as part of the providers' due diligence. In addition, Article 41 of the DSA requires VLOPs and VLOSEs to establish a compliance function that is independent of their operational function and serves as a channel for co-operation with the Commission and the Digital Services

---

[177] Barata and others (n 13) 56.
[178] Cary Coglianese and Evan Mendelson, 'Meta-Regulation and Self-Regulation' in Robert Baldwin, Martin Cave and Martin Lodge (eds), *The Oxford Handbook of Regulation* (OUP 2010) <https://doi.org/10.1093/oxfordhb/9780199560219.003.0008> accessed 12 October 2023.
[179] Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1995).
[180] Neil Gunningham, 'Regulatory Reform and Reflexive Regulation: Beyond Command and Control' in Eric Brousseau, Tom Dedeurwaerdere and Bernd Siebenhüner (eds), *Reflexive Governance for Global Public Goods* (Oxford Academic, The MIT Press 2012) <https://doi.org/10.7551/mitpress/9780262017244.003.0103> accessed 12 October 2023.
[181] Zingales (n 155) 214.

Coordinators. The meta-regulatory framework is also complemented by accompanying obligations, such as a framework for data access for verified researchers, transparency reporting to the general public on risk assessment and identification (in addition to audit and audit implementation reports), and human resources provided by each VLOP and VLOSE provider for content moderation.[182] An additional illustration of the meta-regulatory strategy is the implementation of codes of conduct, which require thorough evaluation to ascertain their suitability and efficacy for the sector.

9. What could be improved?

9.1. Specific provisions of sectoral legislation

The DSA's reference to existing EU legal acts that influence online intermediaries as *lex specialis* – for example, the Video Sharing Platform (VSP) provisions of the Audiovisual Media Services Directive (AVMSD) – is deemed inadequate for definitively ensuring that the peculiarities of online content dissemination are duly considered within the regulation and its oversight. Should the current strategy of instituting a Regulation without establishing supervision structures specifically tailored to online content dissemination, or without stipulating exceptions to prevent the horizontal rules from conflicting with sector-specific provisions, be sustained, then it becomes even more crucial to preserve the function of administrative bodies at the Member State level. These bodies possess the expertise necessary to address these peculiarities. This stance does not affect the potential and necessity for improved cooperation between the authorities and agencies of the Member States.[183]

[182] ibid 217-18.
[183] Cole, Etteldorf and Ullrich (n 1) 223.

9.2. Definition of harmful and illegal content

While the DSA does not specifically address 'harmful' content by providing a definition, it may warrant reconsideration as to whether the regulation should explicitly recognise that Member States have leeway to develop strategies for managing such content. Specifically, this involves controlling its dissemination to mitigate its potential harm, utilising mechanisms that the DSA itself makes available. It has been astutely observed that harmful content presents greater challenges for response in a manner that upholds fundamental rights than illegal content does. This complexity has led the Commission to previously suggest that this matter be tackled through distinct regulatory tools and authorities.[184] The regulatory strategies and techniques for handling illegal content within the DSA could be beneficially adapted for addressing harmful content.

Content moderation is applicable to all types of illegal content without distinguishing between manifestly illegal content and other illegal varieties. Yet, for manifestly illegal content – which is apparent as unlawful to a layperson without detailed content analysis – a distinct content removal process could be contemplated. This might involve expedited timelines, enhanced channels of communication with authorities, and obligations to preserve evidence, similar to those stipulated in the TERREG. A gap remains in defining the jurisdictional reach of content moderation decisions. Since illegal content is also determined according to national laws, content may be deemed illegal in one Member State but not in another. Therefore, it is important to regulate the territorial application of content removal rules within the DSA, as

[184] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Tackling online disinformation: a European Approach' COM (2018) 236 final.

failure to do so may lead to excessive deletions that could endanger freedom of expression in certain locales.[185]

9.3. Complaint handling mechanism

The duty for online platforms to create mechanisms for handling complaints and facilitating out-of-court dispute resolutions constitutes significant procedural protections. The requirements detailed in Articles 20 and 21 are extensive and accentuate the universal character of the rights in need of safeguarding. It is necessary to support the enforcement of these rules with robust and definitive implementation and enforcement actions. Without this, vague terminology such as 'undue delay', 'timely', and 'easy access' may result in inconsistent applications and protracted legal disputes. Given that the DSA does not anticipate the establishment of industry standards in this realm, reliance will be placed on codes of conduct. Nonetheless, the suitability and efficacy of these self-regulatory measures remain uncertain, particularly in a domain so pivotal for users' rights and transparency. The extent to which these requirements will interact with sector-specific national legislation, such as Germany's NetzDG, which already mandates that social media networks implement complaint management systems, also remains to be seen. The expanded procedural framework for trusted flaggers (Article 22) echoes the Commission's preceding views on this issue and provides a much-needed clarification to enhance the efficiency of responses to (trusted) notifications.[186]

Settlement bodies will likely rectify incorrect moderation decisions in numerous instances. Yet, there are multiple ways in which they might fail, such as by delivering conflicting resolutions that incentivise users to engage in forum shopping and result in widespread fragmentation and inconsistency in how platforms' community standards are interpreted. The DSA will also have

[185] Barata and others (n 13) 40.
[186] Cole, Etteldorf and Ullrich (n 1) 197-98.

a global influence in this context. Companies like Facebook and Twitter expanded by being globally accessible, progressively growing into regions with an emerging user base. Their successors will not enjoy the same level of operational leeway. Investors and entrepreneurs across the globe will now have to take into account compliance costs related to gaining users in the EU from the outset, before even contemplating the launch of new platform-based businesses.[187]

9.4. Codes of conduct

The DSA does not herald the discontinuation of codes of conduct; rather, it reinforces their role, as encapsulated in Article 45, by broadening the scope of codes of conduct to encompass all forms of illegal online content. It is important to acknowledge that in numerous instances, the only feasible method to manage systemic risks or to adhere to the regulations formulated through the codes of conduct may necessitate the employment of automated filtering systems. Notwithstanding the transparency requirements specified in the DSA concerning the usage of such tools, it is crucial to recognise that inaccuracies in automated monitoring can have a serious and lasting impact on individuals' fundamental rights, including the right to privacy, freedom of expression and information, protection from discrimination, and the right to a fair process.[188]

Nevertheless, the DSA does not prescribe this self-regulatory model as a universally applicable remedy. This concept should be interpreted alongside the DSA's provisions that pertain specifically to major tech companies, often referred to by the acronym GAFAM. Article 71 details that when a very large online platform presents commitments to adhere to the pertinent clauses of this Regulation, the Commission may, through a formal decision, make such

[187] Keller (n 112) 232.
[188] Barata and others (n 13) 20.

commitments obligatory. Should the VLOP fail to honour its commitments in this context, the Commission has the authority, as per Article 74, to levy fines for non-compliance with a voluntary measure that has been rendered compulsory by virtue of an Article 71 decision.[189]

The empowerment of the Commission in Article 45 to devise codes of conduct for managing systemic risks identified across various VLOPs is a positive move towards a self-regulatory model. However, the language used is somewhat ambiguous and lacks clear details regarding the role of regulators — or in this instance, the Commission and the European Board for Digital Services (EBDS) — which is particularly pertinent given the scepticism surrounding the effectiveness of such codes. In light of the historical ineffectiveness of similar tools to tangibly enhance the accountability of platform operations, a pledge towards a more defined co-regulatory approach would be more favourable. The 'privacy by design' principle within the General Data Protection Regulation, underpinned by technical standards, exemplifies how the aims of protecting fundamental rights can be converted into a more quantifiable and structured legal framework, thereby enabling more robust regulatory monitoring.[190]

9.5. Liability exemption

The exemptions from liability in the DSA remain largely unchanged, now with added explicit requirements for service providers to act on official orders concerning illegal content or to comply with requests for user information. Decoupling the issue of liability (exemption) from the obligation to adhere to the additional (newly introduced) due diligence requirements has its merits, yet the connection between these two components of the DSA warrants further debate. This is particularly true concerning how non-compliance with national law obligations might lead to the provider being deemed liable. The DSA refines the conditions for establishing actual

[189] Jougleux (n 29) 205-06.
[190] Cole, Etteldorf and Ullrich (n 1) 200.

knowledge and sets out uniform procedures for notifications and complaints. Nonetheless, the Recitals relating to the continued 'no general monitoring' mandate may not sufficiently resolve ambiguities around what types of specific actions aimed at limiting content or proactively identifying particular, novel illegal activities are allowed without breaching this mandate. The revised rules in the liability chapter underscore the necessity for courts and authorities to command prompt and uniform reactions from providers, especially in pressing situations. In view of this, the ultimate iteration of the legal framework should clarify that Member States' strategies to handle harmful content (or other sectoral approaches within EU legislation) remain viable, even if the DSA does not directly tackle this subject.[191]

9.6. Compliance monitoring and enforcement

The appropriateness of confining the extensive duties found in Section 4 exclusively to Very Large Online Platforms (VLOPs) is up for debate. In terms of risk management, it is conceivable that online platforms with less than 45 million users may still pose systemic risks. Moreover, most online platforms are already acquainted with fundamental mechanisms such as risk management from other domains, including anti-fraud, information technology security, or data protection. Recommendation systems and automated content moderation, tools used by almost all platforms, especially those dependent on advertising revenue for content distribution, are common. Limiting the obligation to allow access to data for compliance checks solely to VLOPs could prevent researchers from gaining important insights into the potential risks of new business models and content moderation methods. It would be prudent to extend these comprehensive obligations to all (new) online platform providers from the outset, to cultivate a secure and accountable online sphere right from the start. Exemptions should only be considered for certain types of providers if these obligations are proven to be a deterrent to

[191] ibid 38-39.

market entry or cause considerable economic disadvantages.[192] Additionally, the requirement for providers to publish risk assessments, mitigation strategies, and audit reports only three months post-audit could result in delays in identifying potential issues.[193]

In the original argument by Ayres and Braithwaite[194], the critique was aimed at the lack of sufficient independence of compliance officers, who are obliged to notify the regulatory bodies of any non-compliance by management, with the risk of criminal charges looming over them. The DSA, however, does not stipulate such criminal liabilities, nor does it impose particular conditions on the autonomy of the compliance function, potentially undermining the efficacy of this safeguard. Conversely, the DSA does set out more detailed criteria for the independence of auditors. Article 37 specifies that auditors cannot be remunerated through contingency fees, must not have offered non-audit services to the service provider in the preceding year and must abstain from providing such services in the year following the audit. Furthermore, they should not have conducted audits for the service provider or any related legal entity for more than a decade continuously. Nonetheless, it is conceivable that the mere prospect of future audit engagements with the same provider could affect the impartiality of the auditor.[195]

There could be a greater emphasis on leveraging the administrative frameworks within Member States rather than centralising certain powers within the Commission. This approach is not deemed crucial for the DSA's remit, despite being akin to the paradigm used in competition law and the Digital Markets Act (DMA). The same holds for the conception of the new collective entity of national regulators at the EU level – EBDS, which is intended for institutionalised cooperation but is somewhat limited in its decision-making capabilities. The obligation for DSCs to be answerable to their counterparts in other Member States represents

[192] ibid 201.
[193] Zingales (n 155) 220.
[194] Ayres and Braithwaite (n 179) 125.
[195] Zingales (n 155) 221-22.

a significant advance in ensuring effective enforcement in cross-border instances, particularly when differing opinions could lead to procedural repercussions. Yet, a coherence mechanism comparable to that in data protection law, which facilitates cooperation among national supervisory authorities, has not been introduced thus far.[196]

In tackling the systemic risks posed by Very Large Online Platforms (VLOPs), the proposition of incorporating a dedicated and newly established regulatory authority at the EU level could be entertained. The rationale for this centres on efficiency and the extensive cross-border influence of VLOPs. Nonetheless, this transnational aspect alone does not warrant the removal of the customary administrative and procedural self-determination of Member States or the neglect of particular supervisory needs in certain domains, such as the dissemination of content. Thus, any move towards centralisation would require careful coordination with national enforcement authorities. Models for such an arrangement could be inspired by existing entities like the Consumer Protection Cooperation Network (CPC), the Body of European Regulators for Electronic Communications (BEREC), the European Data Protection Board (EDPB), or the European Regulators Group for Audiovisual Media Services (ERGA). These cooperation networks are underpinned by the national competent authorities. A central entity that convenes these national authorities or bodies could address issues necessitating robust international collaboration or those too substantial for a single body to handle. Moreover, a centralised body could offer support to national enforcement agencies and enhance their collaborative efforts.[197]

As evidenced by the General Data Protection Regulation (GDPR), ambitious regulatory content without robust enforcement mechanisms amounts to nothing more than a theoretical construct. The apparent shortcomings in GDPR enforcement have notably shaped the discourse

[196] Cole, Etteldorf and Ullrich (n 1) 40.
[197] ibid 205.

surrounding the enforcement provisions of the DSA. The DSA advocates for a centralised approach to enforcement against the most influential platforms by the European Commission and sets strict timelines for Digital Services Coordinators and the Commission's actions. At the national level, EU member states are tasked with determining the configuration and resourcing of their domestic regulatory authorities. Navigating the complexities of regulatory jurisdiction posed by the DSA will be challenging, given its implications for media law, telecommunications regulations, consumer protection, data protection, intellectual property, and criminal law. Some nations might opt to establish new regulatory bodies, while others may delegate these supervisory responsibilities to existing agencies, either individually or in combination. Practical considerations, historical precedents, and country-specific factors are likely to lead to a diverse array of institutional models for implementing the DSA.[198]

9.7. Online advertising

Article 25 DSA forbids interface designs that mislead or coerce users of the service, or in any significant manner, compromise the users' ability to make free and informed choices. Nevertheless, this prohibition is limited to online platforms, such as Facebook, TikTok, YouTube, or Twitter, and does not extend to websites that, for instance, incorporate Google Ads. More significantly, this ban does not encompass practices that fall within the scope of the GDPR and the Unfair Commercial Practices Directive. This exclusion pertains to all pop-ups that collect personal data, thereby side-lining a vast range of data-collection methods. When it comes to advertising based on surveillance, the DSA partially addresses this with tentative restrictions in Article 26. This article bars online platform providers from showing ads to users based on profiling as outlined in the GDPR, and from utilising 'special categories of personal data' as indicated in Article 9(1) of the GDPR. Similar to interface design restrictions, these

[198] Joris van Hoboken and others, *Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications* (Joris van Hoboken and others eds, Verfassungsblog 2023) 7.

limits are applicable solely to online platforms as categorised by the DSA and do not affect websites, apps, or other intermediary services that integrate services like Google Ads. Moreover, the DSA's restriction only pertains to advertisements displayed by platforms to their users directly. This means providers are still at liberty to position such ads elsewhere on the web, should they offer such a service, not reflecting the realities of the current advertising technology landscape. In practice, the ban in the DSA will not encompass mechanisms like cookies and tracking banners, which are prevalent on most websites through services like Google Ads. Compounding this, Article 26 overlooks the usage of proxy data for sensitive characteristics.[199]

9.8. Role of the European Commission

Aspects that deserve more attention relate in particular to the difference between the European Commission (EC) and a separate independent EU supervisory authority and the tensions associated with the EC's different policy objectives, which could affect the way it carries out its supervisory tasks under the DSA.[200]

Intricate evaluations concerning fundamental rights, such as freedom of expression and the right to privacy, are typically the remit of independent bodies shielded from direct political influence. However, the European Commission is not an autonomous regulatory entity; it is the principal executive organ of the EU. Through its composition and appointment process, it is inherently political, endowed with the privilege of legislative initiation and a pivotal role in legislative negotiations. The DSA's primary policy goals are to foster the digital single market, combat online harms, particularly illegal content, and safeguard fundamental rights on the

[199] 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 and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023) 57-58.
[200] Buri (n 169) 78.

internet. The interplay among these goals is multifaceted, marked by inevitable conflicts necessitating political judgement and ongoing equilibrium. Given these policy goals, the European Commission's stance — as both the executive with a legislative monopoly and the enforcer of the DSA — is equally multifaceted. Various sectors within the Commission (Directorates-General, DGs) chase divergent policy objectives, which can often conflict, typically oscillating between promoting the internal market and prioritising trade, sometimes at the expense of protecting fundamental rights. Consequently, it is improbable that the Commission's enforcement actions and initiatives under the DSA will remain uninfluenced by the institution's broader agenda in areas related to the DSA and other policy domains.[201]

This concept encompasses the restriction on the use of minors' personal data and special categories of data for online advertising purposes (articulated in Articles 26 and 28 of the DSA). In this context, it may prove challenging to ensure the European Commission's impartiality as the primary enforcer for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) whilst simultaneously considering the policy decisions or legislative initiatives that the same body formulates in the realm of data protection law or other associated fields.[202]

A further critical aspect where the Commission's enforcement responsibilities under the Digital Services Act (DSA) could clash with its broader institutional activities is the safeguarding of freedom of expression. The EC has been instrumental in certain initiatives: notably, towards the end of February, it declared a prohibition on the Russian media outlets Russia Today and Sputnik. This declaration was swiftly succeeded by actions from the Council proscribing the broadcast within the EU of media entities deemed as principal instruments of Russian

[201] ibid 79-80.
[202] ibid 81-82.

disinformation. Although the General Court of the European Union upheld these measures[203], experts have cast doubts about the restriction's proportionality and have highlighted concerns regarding its implications for freedom of expression and the accessibility of information within the EU.[204]

The European Commission has also put forward a proposition to establish a mechanism for crisis management to be utilised in extraordinary situations (stipulated in Article 36 of the DSA), which would act as a supplement to the anticipatory and voluntary crisis protocols already envisaged in Article 37 of the DSA. A collective of thirty-eight organisations[205] which advocate for digital rights, has cautioned that 'decisions that affect freedom of expression and access to information, in particular in times of crisis, cannot be legitimately taken through executive power alone'.[206]

9.9. Cost of DSA implementation

The accompanying impact assessment for the Digital Services Act (DSA) suggests that improved harmonisation will bolster digital commerce and enhance the competitiveness of business users, potentially yielding a macroeconomic benefit of approximately 0.3 to 0.4 percent of the EU's GDP.[207] The analysis acknowledges costs, albeit solely the direct compliance expenses, and anticipates no indirect costs arising from the DSA.[208] This perspective is deemed insufficient. Although potential gains from harmonisation are acknowledged, it is also probable that the escalating costs associated with operating and

[203] Case T-125/22 *RT France v Council* [2022] EU:T:2022:483.
[204] Buri (n 169) 85.
[205] EDRi, 'A New Crisis Response Mechanism for the DSA' <https://edri.org/our-work/public-statement-on-new-crisis-response-mechanism-and-other-last-minute-additions-to-the-dsa/> accessed 10 December 2023.
[206] Buri (n 169) 86.
[207] 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.
[208] ibid annex 3 table 2.

utilising platform services will affect users. New regulatory measures invariably impose financial burdens on the operators concerned, with consequent downstream effects. Should such impacts hinder the spread or uptake of novel, innovative technologies, the economic fallout could be significant, with varying implications across different nations and industries.[209]

Smaller firms and less sizable countries, which lack scale benefits, are likely to bear the burden of restrictive regulations more acutely. These smaller nations typically possess reduced absolute advantages, such as data volume and economic expertise, and often have to depend on factors other than scale for competitiveness. To remain competitive, they are compelled to invest more substantially in research and development, intangible assets, and other factors contributing to digital endowments, resulting in greater digital intensity. Consequently, digital regulations can have disparate impacts on businesses, sectors, and countries, influenced by their scale and reliance on digital intermediaries.[210]

The Digital Services Act (DSA) includes several clauses that will engender new administrative and compliance expenditures for online platforms, and it is also expected to induce indirect costs. The likelihood is that it will dampen the appeal of delegating business processes to external entities. The provisions for 'know your customer' will increase the probability of platforms segregating business services linked to their users, leading to direct contracts between user companies and platforms. The obligation for platforms to ensure the traceability of traders is apt to make data services more integral and less likely to be outsourced. Consequently, companies may have reduced motivation to subcontract or relocate such services overseas. Furthermore, this regulation is set to elevate the costs associated with hosting transactions on the platform, and it is the smaller merchants, who contribute minimal revenue

[209] Fredrik Erixon and others, 'After the DMA, the DSA and the New AI Regulation: Mapping the Economic Consequences of and Responses to New Digital Regulations in Europe' (2022) 3 ECIPE Ocassional Paper 24.
[210] ibid 27-28.

to the platform, who are poised to experience the strain. Some platforms may curtail the transaction capabilities of these smaller traders, resulting in market exclusion phenomena and reinforcing the scale benefits enjoyed by larger corporations.[211]

Another global concern that is anticipated to emerge relates to competition. The principal economic concern with the Digital Services Act (DSA) and the Digital Markets Act (DMA) is not the administrative load they impose. Rather, it is the potential restriction of market entry and the consequent services that may become inaccessible or unaffordable. The DSA enforces duties on even the smallest of platforms, responsibilities that today's leading platforms either adopted much later in their lifecycle or did not assume at all. New market entrants will have to assume similar obligations far earlier, facing such obligations once they achieve a mere €10 million in revenue and employ fifty staff.[212] Elevated transaction expenses resulting from digital regulations are likely to increase the costs of intermediary services, which, in turn, has a knock-on effect on intermediate sales downstream. While these costs impact all users, they particularly affect downstream industries that rely on competitively priced services.[213]

10. The new DSA and the rest of the World

The approach of the new Regulation is innovative and has not been previously established in practice. It also does not replicate regulations found in other global regions. The EU is instead positioning itself as a pioneer, and it is anticipated that the regulation will inspire the adoption of similar laws in other major digital markets worldwide. For example, the GDPR was substantially adopted by numerous countries. Furthermore, other EU directives on data and its processing have been 'internationalised' to a certain degree.[214]

---

[211] ibid 33.
[212] Keller (n 112) 230-31.
[213] Erixon and others (n 209) 34.
[214] ibid 4.

In contrast to the regulation of conventional hate speech, the regulation of online hate speech typically is not feasible to be separated either technically or financially. An examination of the standard terms and conditions of IT firms reveals that these companies commonly adopt a uniform definition across the globe. Generally, the provisions set by Europe are mirrored in the international terms and conditions of these corporations, thereby applying to their operations on a global scale.[215]

Furthermore, the world's largest platforms are anticipated to implement certain specific measures to shield users, including the enhancement of tools to facilitate dialogue between claimants and respondents within notice and response frameworks. Transformations introduced as part of the efforts by VLOPs to curtail risk, as mandated by Article 35, are expected to have worldwide repercussions. This also includes more tangential advantages that will emerge from provisions such as improved data accessibility for researchers, as laid out in Article 40.[216]

Notwithstanding valid critiques, the Digital Services Act (DSA) has the capacity to set a worldwide benchmark. There's considerable global attention, notably from the United States, but also from nations like Brazil, Pakistan, and Japan. As the inaugural democratic continent to put forward a thoroughly deliberated statute, Europe stands poised to navigate the course and safeguard the Internet from domination by surveillance-centric corporations. Vigorous and uniform enforcement at both the EU level and within Member States will be vital for triumph.[217]

Equally, one must not overlook a secondary manifestation of the Brussels effect, pertaining to the potential of regulated entities themselves extending the compliance frameworks established under the DSA to territories beyond the EU. This might significantly enhance the interaction

[215] Bradford (n 68) 164.
[216] Keller (n 112) 229.
[217] Geese (n 36) 72-73.

between platforms and regulatory bodies internationally, yet without adequate institutional support, it poses the dual hazard of selective implementation and inadequate sensitivity to the local context. To avert such an outcome, it is imperative to guarantee that the intricacies of meta-regulation are properly conveyed and comprehended. This begins with an acknowledgment that the due diligence obligations placed upon providers are not standalone; they are components of an expansive ecosystem intended to foster suitable experimentation, observation, and regulatory discourse, with potential progression to enforcement measures. Importantly, this infrastructure must incorporate stringent supervisory and accountability mechanisms to fulfil its objectives.[218]

11. Conclusion

Over the past two decades, technologies and business models have advanced, and the EU framework is finding it challenging to address liability concerns presented by new entities like search engines, social networks, or online marketplaces. Additionally, changes in societal challenges have altered the nature and magnitude of the problem, with the emergence of a variety of harmful online practices such as the spread of terrorist content online, the increased use of platforms for the distribution of counterfeit goods, and the proliferation of false or misleading news and online advertisements.

In the realm of digital market society, the wealth of available information has exponentially increased due to a surge in the number of ‘channels’ on the supply side. These channels are further bolstered by self-generated information content – stemming not solely from journalistic outlets but from a vast, diverse cosmos. This expansion is championed by many intellectuals as the quintessential manifestation of informational and expressive liberty, giving rise to

[218] Zingales (n 155) 223-24.

ubiquitous external pluralism born from the rivalry among alternative sources in the free market of ideas, which, in this theoretical model, is deemed to ultimately unveil the truth.[219]

There was a prevalent belief that the digital ecosystem could – and should – self-regulate devoid of extraneous (public) oversight. Nonetheless, upon examining the various forms of digital intermediation and 'sharing economies', it becomes evident that the digital ecosystem is fraught with significant disparities in information access, economic might, and negotiation leverage, necessitating vigilant scrutiny and, where appropriate, judicious intervention by public regulators.[220]

The Digital Services Act (DSA) augments and modernises the foundational tenets of the e-Commerce Directive established in 2000, delineating a comprehensive legal framework for the delivery of digital services within the EU by stipulating explicit duties and accountability for intermediary service providers, contingent on their function, magnitude, and influence within the digital sphere. It represents the apex of an extensive development of the liability regime for online intermediaries. Specifically for online platforms, the legislation ushers in profound practical changes: it formalises the content moderation process, imposes stringent oversight of platform operations, and, notably, institutes a new and broadened duty of care that extends the parameters of the safe harbour provisions to their utmost limits.[221] Moreover, the DSA does not supplant sector-specific legislation; rather, it enriches it by serving as an overarching *lex specialis* that spans across all economic sectors in relation to digital services and online intermediaries. Concurrently, efforts are being channelled towards the Digital Markets Act (DMA), which seeks to elevate the degree of competition in European digital marketplaces by

[219] Manganelli and Nicita (n 4) 21-23.
[220] ibid 53.
[221] Jougleux (n 29) 181.

curbing the monopolistic tendencies of dominant firms and facilitating market entry for emergent entities.[222]

The DSA introduces mechanisms to gain insights into the workings of digital platforms. It mandates that particularly extensive platforms conduct risk assessments to pinpoint, scrutinise, and evaluate systemic risks emanating from their services within the EU, including risks associated with algorithmic processes. These platforms are obliged to evaluate all substantial systemic risks presented by their services annually. This encompasses the spread of both illegal content and material that, while not illegal, may still be detrimental. These evaluations must consider the impact of their content moderation frameworks on the identified systemic risks. Following such assessments, the platforms must implement suitable, proportionate, and effective corrective measures — such as modifications to content moderation practices — that are specifically tailored to the identified systemic risks. Moreover, the European Commission is empowered to provide overarching recommendations concerning specific risks, especially to showcase best practices and suggest potential courses of action.

Upon detailed examination, the DSA's prioritisation of process over substance also gives rise to numerous unresolved issues. The finalised version of the regulation is marked by a series of trade-offs, such as those related to alternative dispute resolution, as well as noticeable omissions, notably the absence of a clear mandate for resolving disputes that arise from content moderation practices. Nonetheless, the DSA introduces significant procedural enhancements, notably refining the mechanisms for notification and action and the articulation of reasons.[223]

Despite certain limitations and exclusions, the DSA appears to align with the needs articulated by consumer groups and the necessities of EU citizens. These necessities are growing in

[222] Menkes (n 2) 48.
[223] Ortolani, 'If You Build it, They Will Come: The DSA 'Procedure Before Substance' Approach' (n 126) 162.

urgency due to the increased risks associated with the spread of illegal and harmful content, the availability of unsafe products, skewed access to information, and certain constraints on informed decision-making or freedom of speech.[224]

The prevailing presumption appears to be that Europe's economies will uniformly react to the implementation of the DSA. Yet, this is improbable; it is sensible to anticipate that the impact of this regulation will differ significantly across countries due to the substantial variances among European economies in their digital economy assets, the intensity of their use of digital services, and the degree to which they host digital intermediaries. Regulations affecting platforms that influence the growth and conduct of these platforms will have a more pronounced effect in countries where digital services are extensively utilised and produced, as opposed to those where the use and production of digital services are less pronounced.[225]

The DSA and DMA regulations are a cause for optimism as they promise to establish a lasting legal infrastructure for the digital domain at the conclusion of the legislative journey. They may empower the EU to establish benchmarks, similar to the successes seen in data protection. These regulations are commendable for their ambition, targeting not just intermediaries at large but also designating specific categories of providers that play a pivotal role in linking businesses and consumers, who will subsequently undergo meticulous scrutiny as gatekeepers or will have to meet additional prescribed duties. The scope of the regulations and the jurisdiction are set to extend beyond the geographical establishment of the involved providers within the EU, sending a significant message to the marketplace. Assuming that this new regulatory environment will endure and shape the digital intermediary market for the forthcoming decade at least, these new rules are seen as a solid foundation.[226]

---

[224] Manganelli and Nicita (n 4) 194.
[225] Erixon and others (n 209) 6.
[226] Cole, Etteldorf and Ullrich (n 1) 41-42.

The official release of the DSA concludes a prolonged period of drafting and negotiation, heralding a new era focused on enforcement, practical accessibility to legal redress, and the capacity to establish international benchmarks. The depiction of the DSA as Europe's 'digital constitution', crafted to assert the supremacy of democratically established regulations over the private international regulatory frameworks of major technology firms, should be rigorously examined. While it perpetuates the foundational principles of the e-Commerce Directive for the governance of online services dealing with third-party content and formalises the existing self-regulatory practices of online platforms, it also ushers in significant legal advancements. These include a graduated framework of due diligence for intermediary services, the governance of content moderation through the application of service terms, mandatory systemic risk assessments for widely utilised platforms and search engines, and researcher access to data. In essence, with the DSA, the European Union aspires to once again pioneer a global regulatory standard for the digital landscape.[227]

[227] van Hoboken and others (n 198) 5.

12. Bibliography

Ambroziak AA, ‘EU’s Perspective on the Functioning of Giant Online Platforms in the Digital Economy’ in Dąbrowski LD and Suska M (eds), *The European Union Digital Single Market: Europe's Digital Transformation* (Taylor & Francis Group 2022)

Ayres I and Braithwaite J, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1995)

Barata J and others, *Unravelling the Digital Services Act Package* (European Audiovisual Observatory 2021)

Becker S and Penfrat J, ‘The DSA Fails to Reign in the Most Harmful Digital Platform Businesses – But It Is Still Useful’ in van Hoboken J and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023)

Bradford A, *The Brussels Effect: How the European Union Rules the World* (OUP 2020)

Buri I, ‘Regulator Caught Between Conflicting Policy Objectives: Reflections on the European Commission’s Role as DSA Enforcer’ in van Hoboken J and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023)

Castillo APD, ‘The Digital Services Act package: Reflections on the EU Commission’s policy options’ (2020) 12 ETUI Policy Brief

Coglianese C and Mendelson E, ‘Meta-Regulation and Self-Regulation’ in Baldwin R, Cave M and Lodge M (eds), *The Oxford Handbook of Regulation* (OUP 2010) <https://doi.org/10.1093/oxfordhb/9780199560219.003.0008> accessed 12 October 2023

Cohen JE, ‘The Regulatory State in the Information Age’ (2016) 17 Theoretical Inquiries in Law 369

Cole MD, Etteldorf C and Ullrich C, *Updating the Rules for Online Content Dissemination: Legislative Options of the European Union and the Digital Services Act Proposal* (Nomos Verlag 2021)

EDRi, ‘A New Crisis Response Mechanism for the DSA’ <https://edri.org/our-work/public-statement-on-new-crisis-response-mechanism-and-other-last-minute-additions-to-the-dsa/> accessed 10 December 2023

Erixon F and others, ‘After the DMA, the DSA and the New AI Regulation: Mapping the Economic Consequences of and Responses to New Digital Regulations in Europe’ (2022) 3 ECIPE Ocassional Paper

European Union Agency for Fundamental Rights, *Handbook on European Law relating to Access to Justice* (Publications Office of the European Union 2016)

Geese A, ‘Why the DSA Could Save Us From the Rise of Authoritarian Regimes’ in van Hoboken J and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023)

Goanta C, ‘Now What: Exploring the DSA’s Enforcement Futures in Relation to Social Media Platforms and Native Advertising’ in van Hoboken J and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023)

Gunningham N, ‘Regulatory Reform and Reflexive Regulation: Beyond Command and Control’ in Brousseau E, Dedeurwaerdere T and Siebenhüner B (eds), *Reflexive Governance*

for Global Public Goods (Oxford Academic, The MIT Press 2012) <https://doi.org/10.7551/mitpress/9780262017244.003.0103> accessed 12 October 2023

Jaursch J, 'Platform Oversight: Here is what a Strong Digital Services Coordinator Should Look Like' in van Hoboken J and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023)

Jougleux P, *Facebook and the (EU) Law: How the Social Network Reshaped the Legal Framework* (Springer International Publishing 2022)

Kawecka-Wyrzykowska E, 'Proposal for an EU Digital Levy: Challenges and Possible Implications' in Dąbrowski LD and Suska M (eds), *The European Union Digital Single Market: Europe's Digital Transformation* (Taylor & Francis Group 2022)

Keller D, 'The European Union's New DSA and the Rest of the World' in van Hoboken J and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023)

Kenney M and Zysman J, 'The Rise of the Platform Economy' (2016) 32 Issues in Science and Technology 61-69

Kuczerawy A, 'Remedying Overremoval' in van Hoboken J and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023)

Madiega T, *Reform of the EU Liability Regime for Online Intermediaries: Background on the Forthcoming Digital Services Act* (European Parliamentary Research Service 2020)

Manganelli A and Nicita A, *Regulating Digital Markets: The European Approach* (Springer International Publishing 2022)

Mantelero A, 'Fundamental Rights Impact Assessment in the DSA' in van Hoboken J and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023)

Menkes J, 'Freedom of Speech in the Age of Digitalisation: Opportunities and Threats' in Dąbrowski LD and Suska M (eds), *The European Union Digital Single Market: Europe's Digital Transformation* (Taylor & Francis Group 2022)

Moss D, Gundlach G and Krotz R, 'Market Power and Digital Business Ecosystems: Assessing the Impact of Economic and Business Complexity on Competition Analysis and Remedies' SSRN Electronic Journal <https://ssrn.com/abstract=3864481> accessed 15 December 2023

Mulligan DK and Bamberger KA, 'Saving Governance-By-Design' (2018) 106 California Law Review 697

Ortolani P, 'The Three Challenges of Stateless Justice' (2016) 7 Journal of International Dispute Settlement 596

—— 'If You Build it, They Will Come: The DSA 'Procedure Before Substance' Approach' in van Hoboken J and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023)

Ranganathan N, 'Regulating Influence, Timidly' in van Hoboken J and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023)

Roosevelt F, ‘The Four Freedoms’ <https://www.archives.gov/milestone-documents/president-franklin-roosevelts-annual-message-to-congress> accessed 20 November 2023

Steering Committee for Media and Information Society, *Content Moderation, Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation* (Council of Europe 2021)

van Hoboken J and others, *Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications* (van Hoboken J and others eds, Verfassungsblog 2023)

Wilman F, ‘Between Preservation and Clarification: The Evolution of the DSA’s Liability Rules in Light of the CJEU’s Case Law’ in van Hoboken J and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023)

Zingales N, ‘The DSA as a Paradigm Shift for Online Intermediaries’ Due Diligence: Hail To Meta-Regulation’ in van Hoboken J and others (eds), *Putting the DSA Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023)