# EUROPE'S DIGITAL REVOLUTION: THE DSA, THE DMA, AND COMPLEMENTARY REGIMES

# TOPIC II – GENERAL INTRODUCTION

*P.J. Loewenthal*
*C. Sjödin*
*F. Wilman**

At the end of 2022, two pieces of landmark legislation regulating the provision of certain digital services in the European Union ("EU") – the Digital Services Act ("DSA")[1] and the Digital Markets Act ("DMA")[2] – were adopted. Two years following their entry into application, the present Report aims to analyse this new regulatory framework and take stock of the first experiences gathered in its application, as well as to map the broader regulatory context in which to place that framework. To that aim, this report consists of three parts. Part I examines the DSA and the DMA as a whole and places them alongside the various complementary EU legal regimes that regulate the provision of digital service in the EU. Part II focuses specifically on the DSA, while Part III focuses specifically on the DMA.

## PART I: GENERAL OVERVIEW AND COMPLEMENTARY REGIMES

### A. Introduction

While the DSA and the DMA pursue different objectives, vary in their scope of application, and are likely to have a different impact on European society, they share common origins and features. The rules that those acts lay down were in fact meant to form part of a single legislative instrument regulating the provision of digital services in the EU, but the aforementioned divergences rendered such an approach impractical. The consequence is two separate acts whose main common feature is that they redefine the regulatory landscape for

* P.J. Loewenthal and F. Wilman, who drafted Parts I and II respectively, are both Members of the Commission Legal Service. C. Sjödin, who drafted Part III of this Report, is a former Member of the Commission Legal Service and currently deputy head of unit in the Commission's Directorate-General for Competition. This Report takes account of developments until 15 February 2025. All views expressed in this Report are purely personal.

[1] 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) (OJ L 277, 27.10.2022, p. 1).

[2] 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) (OJ L 265, 12.10.2022, p. 1).

providers of digital services in the EU, tilting the balance of the relationship in favour of users.

The first part of this report explores the convergences and divergences between the DSA and the DMA, while placing those acts within the broader regulatory framework governing the provision of digital services in the EU. It begins by exploring the economic and regulatory climate within which those acts were adopted. It then examines the common legislative origins of those acts, turning to the divergences in objectives and obligations, which explains the differing scopes of application of each act and their expected impact on society. It also compares the new supervision and enforcement frameworks created by those acts, and explains how those acts will apply alongside other acts regulating the provision of digital services in the EU, many of which were only enacted after the DSA and the DMA came into force.

## B. Europe's digital deficit

Europeans are often accused of over-regulation. "While Americans innovate, Europeans regulate" is an oft-repeated refrain. Europe's seeming failure to reap the benefits of the technology revolution following the launch of the Internet is cited as a case in point. Of the top-ten tech companies in the world as measured by total revenues, eight are American, two are Chinese, and none are European. Of the top-fifty tech companies worldwide, only four are European.[3] It is this lack of tech companies which best explains the divergent economic fortunes of the United States ("U.S.") and the EU since the start of the new millennium.[4] Europeans' regulatory zeal – so the argument goes – must therefore explain the lack of innovation in digital services, which cannot thrive in an environment hostile to business.

Yet, when it comes to digital services, the EU barely regulated their provision until very recently. In fact, prior to 2019, only one EU law directly regulated the provision of such services: the e-Commerce Directive of 2000.[5] What is more, that directive took a hands-off approach to such regulation. Giving effect to the freedom to provide services, the e-Commerce Directive is based on the "country-of-origin" (or "home State control") principle, according to which providers of information society services established in the EU need only comply with the rules on such services in the Member State in which they are established (the

[3] M. Draghi, *The future of European competitiveness*, September 2024, p. 5.

[4] Ibidem, p. 20: "The key driver of the rising productivity gap between the EU and the US has been digital technology ("tech") – and Europe currently looks set to fall further behind. […] In fact, if we exclude the tech sector, EU productivity growth over the past twenty years would be broadly at par with the US […]. Europe is lagging in the breakthrough digital technologies that will drive growth in the future."

[5] 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") (OJ L 178, 17.7.2000, p. 1).

Member State of establishment) in order to provide their services in all other Member States.[6] The flipside of that principle is that other Member States are prohibited from imposing general obligations on those providers that restrict their freedom to provide their services in those Member States (the Member States of destination).[7] In addition, the e-Commerce Directive introduced exemptions from liability for intermediary service providers which, subject to certain conditions and exceptions, shielded them from being held liable for the content uploaded to their service by users, however harmful that content may be.[8] Finally, that directive introduced a prohibition on general monitoring obligations, which means that the Member States were prohibited from obliging, in a general manner, providers of intermediary services to assess whether content uploaded to their services complied with the law prior to that uploading.[9]

If anything, the e-Commerce Directive was actually the biggest obstacle to national digital market regulation in the EU during the past quarter century.[10] Member States that wished to address the societal and competitive harms associated with the provision of digital services were severely limited in adopting measures regulating such services in relation to providers not established in their territory, however noble the objectives pursued or problematic the harms that those measures sought to address. The e-Commerce Directive only permitted those Member States to adopt *ad hoc* measures, subject to stringent substantive and procedural requirements with which most measures with even the most noble objectives had difficulty complying.[11]

Similarly, it was only from the late 2010s onwards that the practices of digital service providers were seriously scrutinised under the EU antitrust rules. Apart from the seminal Microsoft decision of 2004,[12] the Commission's application of the antitrust rules to prominent digital service providers only began in earnest a few years before the Commission's DMA proposal, with three decisions fining Google for various anticompetitive practices in the late 2010s,[13]

---

[6] Art 3(1) e-Commerce Directive.

[7] Art 3(2) e-Commerce Directive.

[8] Arts 12 to 14 e-Commerce Directive.

[9] Art 15 e-Commerce Directive.

[10] A case in point is Case C-376/22, *Google Ireland and Others*, EU:C:2023:835, in which the Court held that an Austrian law requiring providers of online platforms operating in Austria to have a notice and action mechanism in place was incompatible with the country-of-origin principle. A case currently pending before the Court is Case C-188/24, *WebGroup*, which deals with the question whether French legislation penalising the distribution of pornography to minors constitutes an impermissible restriction in relation to the Czech-based pornography platform XVideos.

[11] Art 3(4) e-Commerce Directive.

[12] Commission Decision C(2004) 900 final of 24 May 2004 relating to a proceeding pursuant to Article 82 of the EC Treaty and Article 54 of the EEA Agreement against Microsoft Corporation.

[13] Commission Decision C(2017) 4444 final of 27 June 2017 relating to proceedings under Article 102 TFEU and Article 54 of the EEA Agreement (Case AT.39740 – Google Search (Shopping)); Commission Decision C(2018) 4761 final of 18 July 2018 relating to a proceeding under Article 102 TFEU and Article 54 of the EEA Agreement (Case AT.40099 – Google Android); and Commission Decision C(2019) 2173 final of 20 March 2019 relating to a proceeding under Article 102 TFEU and Article 54 of the EEA Agreement (Case AT.40411 – Google Search (AdSense)).

a commitment decision in relation to Amazon[14] adopted in 2022 and decisions fining Apple[15] and Meta[16] for anticompetitive conduct in 2024.

In short, Europeans' alleged regulatory zeal cannot explain the lack of EU companies among the top tech companies worldwide. That there is a lack of EU companies among the top providers of digital services worldwide does not detract from the fact that Europeans rely heavily on such services. This is true both for European citizens and businesses. The top-ten tech companies worldwide are often the top-ten providers of digital services in the EU. Google Search, Amazon Store, Apple's App Store, Facebook, Instagram, TikTok and X (formerly Twitter) command an important share of their respective markets in the EU and have become a ubiquitous part of Europeans' lives. The providers of those services have generated considerable revenues in Europe, in some cases more than in their home countries. European residents rely on those services for much of their information, goods, and services, and European businesses rely on those services to reach European consumers.

For over a decade, those digital services have had a profound impact on European society, some, but not all of it, good. It is in response to several high-profile cases demonstrating the societal and competitive harms that accompany the provision of digital services in the EU that Europeans have finally demanded their representatives to hold providers of those services accountable for their (in)actions and the resulting harms. That is where the DSA and the DMA come in. However, while the DSA and the DMA mark a distinct change in the regulatory environment applicable to the provision of digital services in the EU, many of the concepts and tools that they deploy are already well known to regulators and the industry.

The DSA is the successor to and was inspired by several soft-law instruments adopted in the late-2010s that sought to address certain societal harms to which the provision of specific digital services give rise. The European Commission's initial forays into the area that would later be governed by the DSA began by emphasising self-regulation and voluntary codes of conduct,[17] but quickly turned to contemplating legislative solutions to address those societal harms.[18]

---

[14] Commission Decision C(2022) 9442 final of 20 December 2022 relating to a proceeding under Article 102 TFEU and Article 54 of the EEA Agreement (Case AT.40462 - Amazon Marketplace and AT.40703 – Amazon Buy Box).

[15] Commission Decision C(2024)1307 final of 4 March 2024 (Case AT.40437 – Apple – App Store Practices (music streaming))

[16] See Commission Press Release, "Commission fines Meta €797.72 million over abusive practices benefitting Facebook Marketplace," 13 November 2024.

[17] Commission Communication "A Digital Single Market Strategy for Europe (COM/2015/0192 final)" and Communication "Online platforms in the Digital Single Market – Opportunities and Challenges for Europe" (COM/2016/0288 final).

[18] See Commission Communication "Tackling Illegal Content Online – Towards and Enhanced Responsibility of Online Platforms" (COM/2017/0555 final) and Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online (OJ L 63, 6.3.2018, p. 50).

As for the DMA, the excessive duration of antitrust investigations and the high burden of proof to establish infringements of the competition rules drove the search for a "new competition tool" that was meant to bring certainty through *ex ante* regulation. Given the rapid pace of innovation by which digital markets are characterised, the choice was made to devise that tool to bring contestability and fairness to those markets. The resulting prohibitions and obligations imposed by the DMA on gatekeepers operating in EU digital markets essentially correspond to those practices which had been found to be anticompetitive time and again and for which there were no conceivable efficiency defences.

All this means that the DSA and the DMA should not be seen as a radical break with the past. The doctrine and case-law that has developed in relation to the notions and practices which the DSA and DMA have made their own remain relevant for the future, but new ground will be broken, particularly in relation to notions and practices that are new or broadly defined.

## C. Common origins

At their heart, the DSA and the DMA serve a common purpose: to regulate the provision of digital services in the EU. This also explains why both acts share the same legal basis: Article 114 of the Treaty on the Functioning of the European Union ("TFEU"). Unlike EU legislation regulating the provision of digital services before it, the DSA is not merely about removing barriers to the cross-border provision of digital services, nor is the DMA simply *ex ante* competition law enforcement in digital markets.

Article 114 TFEU allows the European Parliament and the Council to adopt legislative acts which have as their objective the establishment and functioning of the internal market. Unlike Articles 53 and 62 TFEU, which allow the EU legislature to adopt directives for the purpose of removing impediments to the taking-up and pursuit of the cross-border provision of services, and Articles 101 and 102 TFEU, which allow the Commission to sanction anti-competitive conduct, Article 114 TFEU allows the EU legislature to regulate the conditions under which the exercise of cross-border economic activities, of which the provision of digital services clearly qualifies, takes place in the EU. In other words, the DSA and the DMA should be compared to any other regulation of economic activity in the EU, for example, similar to telecoms, banking, and transport regulation.

However, whereas telecom and transport regulation are primarily about liberalising previously State-operated markets, the DSA and the DMA, like banking regulation, should be seen as a response to the societal and competitive harms that have been identified and studied over the past two decades as emanating from the provision of digital services. Several high-profile cases

concerning certain digital services have brought those harms to the fore: the Cambridge Analytica scandal, the whistleblower Frances Haugen's revelations about Facebook's deliberate failure to protect teenagers using its service, Epic Game's challenge to Apple's profiteering by charging exorbitant fees for hosting its apps on the App Store, and Amazon's practices of collecting and leveraging customer data from its business users. These are but a handful of pertinent examples of where legislative action was considered necessary to protect Europeans citizens and businesses using digital services.

The DSA and the DMA should also be seen as a response to increasing legislative action at national level. Notwithstanding the restrictions placed by the e-Commerce Directive and the competition law provisions of the TFEU on national legislative action, numerous Member States began regulating digital services at national level, sometimes in disregard of those restrictions. This further explains the EU legislature's recourse to Article 114 TFEU as the legal basis for the DSA and the DMA. Both acts lay down fully harmonised rules for the provision of the digital services that they cover in the EU and thus seek to prevent the emergence of 27 different regulatory regimes and excessive administrative burdens for digital service providers wishing to operate in the EU.[19]

At their inception, the DSA and the DMA were conceived in the Commission's 2020 Work Programme[20] as a single legal instrument to regulate the provision of digital services. This idea of a single legislative act regulating both the content moderation practices of online intermediaries and the business practices of digital service providers was further reflected in the Commission's Communication "Shaping Europe's Digital Future."[21] The European Parliament followed suit with its legislative own-initiative report proposing a single "Digital Services Act."[22] However, it quickly became clear that the divergent ob-

[19] See Rec. 9 DSA and Art. 1(5) DMA.

[20] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission Work Programme 2020: A Union that Strives for More, COM/2020/37 final, section 2.2 ("*Digital Services Act [that] will reinforce the single market for digital services and help provide smaller businesses with the legal clarity and level playing field they need*").

[21] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Shaping Europe's Digital Future, COM/2020/67 final (That communication describes the content of a future "Digital Services Act Package" as including "ex ante rules to ensure that markets characterised by large platforms with significant network effects acting as gate-keepers, remain fair and contestable for innovators, businesses, and new market entrants" (Section 2.B) and "[n]ew and revised rules to deepen the Internal Market for Digital Services, by increasing and harmonising the responsibilities of online platforms and information service providers and reinforce the oversight over platforms' content policies in the EU" (Section 2.C).

[22] See European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), P9_TA(2020)0272. In that report, the European Parliament "welcome[d] the Commission's commitment to submit a proposal for a Digital Services Act package ('DSA'), which should consist of a proposal amending the E-Commerce Directive and a proposal for ex ante rules on systemic operators with a gatekeeper role" (para 1).

jectives and obligations, the divergent scopes of application, and the divergent supervisory and enforcement regimes would require two separate legislative acts due to their divergent objectives and obligations, their divergent scopes of application and their divergent supervisory and enforcement frameworks.

## D. Divergent objectives and obligations

The objective of the DSA is "to contribute to the proper functioning of the internal market for intermediary services by setting out harmonised rules for a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected."[23] The novelty of the DSA, as compared to the e-Commerce Directive, is that it places certain responsibilities on providers of intermediary services. Such providers are in a unique position in relation to the content displayed on their online interfaces, since they are neither the author of that content, nor are they responsible for uploading it to those interfaces. As the Court describes it, "the role played by [such an] operator is neutral, that is to say, […] its conduct is merely technical, automatic and passive, which means that it has no knowledge of or control over the content […]."[24]

Whereas the e-Commerce Directive sought to enhance the cross-border provision of services in the EU by restricting the ability of Member States to adopt national regulatory barriers and conditionally exempting the liability of intermediary service providers where they have no knowledge or control over the content displayed on their online interfaces, the DSA seeks, in particular, to prevent the spread of illegal and harmful content online by placing "due diligence" obligations on such providers in relation to the services that they provide. It does so by prescribing certain mechanisms that intermediary service providers should put in place and certain actions that they should take to minimise the risk of disseminating illegal and harmful content through their services.

By contrast, the objective of the DMA is "to contribute to the proper functioning of the internal market by laying down harmonised rules ensuring for all businesses, contestable and fair markets in the digital sector across the Union where gatekeepers are present, to the benefit of business users and end users."[25] In essence, that legal instrument seeks to create a level playing field on the market for digital services by imposing ex ante prohibitions and obligations on "gatekeepers" with the ultimate aim of promoting innovation and enhancing consumer choice. Some of those prohibitions and obligations find their genesis

[23] Art. 1 DSA.

[24] Joined Cases C-682/18 and C-683/18, *YouTube and Cyando*, EU:C:2021:503, para 106.

[25] Art. 1 DMA.

in the Commission's competition law case practice, but others are entirely new. By defining the core platform services to which those prohibitions and obligations apply in advance, all the complexity of defining relevant markets in competition law cases was eliminated from the regulatory equation: once an undertaking is designated as a gatekeeper, certain practices in relation to certain core platform services are per se prohibited. In short, the DMA seeks to prevent the largest providers of certain digital services from leveraging their gatekeeper status over those services by obstructing business users using those services to reach their customers directly.

These diverging objectives explain, to a large extent, the divergent content of the obligations imposed by each of those acts, the providers to which they are addressed, and the persons that they are meant to benefit.

The DSA's aim to prevent the dissemination of illegal and harmful content online is meant primarily for the benefit of recipients of intermediary services, but also for those persons affected by those services, even if they have not used them. Consequently, the due diligence obligations that the DSA imposes on providers of such services are primarily aimed at their content moderation practices.[26] The DSA does not define what content is illegal, nor does it oblige providers to remove illegal content from their services; rather, it obliges providers to put in place certain procedural mechanisms to ensure that recipients can notify illegal content to them and that recipients are in turn notified of the action providers have taken in relation to that content. The DSA also seeks to enhance the transparency of intermediary services to the benefit of their recipients and persons affected by those services by requiring providers to set up points of contact, include certain information in their terms and conditions, publish reports and perform audits.[27] Finally, the DSA contains a handful of due diligence obligations constituting absolute prohibitions of certain practices, such as dark patterns and profiling minors.[28]

The DMA's aim to ensure fair and contestable markets for digital services is meant first and foremost for the benefit of business users, which is meant to enhance consumer choice, thus ultimately benefitting end users. To achieve that aim, the DMA contains two lists of obligations for gatekeepers,[29] although some of those "obligations" are in fact framed as prohibitions. The purpose of those separate lists is in fact to make clear that only the second list may be subject to the specification procedure described in Part III of this Report.[30] In addition, the DMA requires gatekeepers to report on the measures that they have adopted to ensure compliance with the prohibitions and obligations, to inform the Commission of planned concentrations even if they fall outside the notification requirements in the Merger Regulation, and to submit themselves

[26] See, e.g., Arts. 14, 16, 17, 23, 28, 34 and 35 DSA.
[27] See, e.g., Arts. 11, 12, 14, 24, 26, 27, 30 to 32, 37 to 40 and 42 DSA.
[28] See, e.g., Arts. 25, 26 and 28 DSA.
[29] Arts. 5 and 6 DMA.
[30] Art. 8 DMA.

to an audit of any techniques for profiling of consumers that it applies.[31]
An overview of these obligations leaves the impression that while the DSA focuses primarily on procedure (establishing redress mechanisms, transparency, and reporting), the DMA focuses primarily on substance (prohibitions of specific anti-competitive conduct). These diverging obligations and, most important, the diverging persons that they are meant to protect (society as a whole vs. business and end users) help explain why a single legislative act covering both the DSA and the DMA would have been impractical and unwieldy. The same is true for the DSA's and DMA's diverging scopes of application.

## E. Divergent yet intersecting scopes of application

While the DSA and the DMA pursue different objectives, they will often apply to the same digital service providers and to the same digital services. Nevertheless, the DSA and DMA have different scopes of application.

### E.1. Material scope of application

The DSA only applies to the provision of one specific type of digital service, namely the provision of "intermediary services." By contrast, the DMA applies to ten categories of "core platform services" ("CPSs"), five of which are covered by the DSA's material scope of application, whereas the others are of a different nature to the intermediary services covered by the DSA. What is more, the DSA and the DMA contain different definitions of intermediary/intermediation services.
Article 3(i) DSA defines "intermediary services" by incorporating the descriptions of the three types of intermediary services that benefitted from an exemption from liability under the e-Commerce Directive.[32] From that definition it follows that the notion of "intermediary services" used in the DSA is limited to "mere conduit," "caching" and "hosting" services. Article 3(i) DSA introduces the new notion of "online platform," which is a type of hosting service. Certain provisions of the DSA also apply to online search engines, a term which is defined in Article 3(j) DSA, but whose relationship with the three intermediary services covered by the DSA is unclear. While Article 3(j) defines online search engines as a type of intermediary service, it does not specify which type. Nor is that apparent from the definitions in Article 3(i) DSA. That classification is important, given the graduated approach to the due diligence obligations imposed on intermediary service providers, with hosting

[31] Arts. 11, 14, and 15 DMA.

[32] Arts. 12-14 e-Commerce Directive, which the DSA has repealed and replaced (Arts. 4 to 6 DSA)

service providers being subjected to more exacting obligations than caching service providers.

By contrast, Article 2(5) DMA defines "online intermediation services" by reference to the definition in Article 2(2) of the Platform-to-Business ("P2B") Regulation.[33] That latter definition requires three cumulative elements to be fulfilled: (i) the service must be an "information society service"; (ii) the service must allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded; and (iii) the service must be provided to business users on the basis of contractual relationships. Only the first of those three elements is a necessary condition for a service to constitute an "intermediary service" within the meaning of Article 3(i) DSA. Rather, the notion of "online intermediation service" in the DMA comes closest to the notion of "online platforms allowing consumers to conclude distance contracts with traders" used in the DSA, which are subject to special due diligence obligations under that act.[34]

The DMA's reference to the P2B Regulation for the definition of online intermediation services makes sense insofar as DMA's objective aligns to a certain extent with that of the P2B Regulation, which is, *inter alia*, "to ensure that business users of online intermediation services […] are granted appropriate transparency, fairness and effective redress possibilities."[35] This also explains the divergence with the DSA's definition, given that the aim of that act is primarily to protect all users from the societal harms to which an intermediary service may give rise, not business users specifically.

The DMA also applies to online search engines, online social networking services, and video sharing platforms. The latter two services will generally qualify as hosting services and online platforms, and thus intermediary services, within the meaning of the DSA. The former is defined by reference to the definition of online search engines in the P2B Regulation, which is largely identical to the definition for online search engines in Article 3(j) DSA, except that the P2B Regulation defines such services as "digital services," whereas the DSA defines them as "intermediary services."

Aside from intermediation services and online search engines, the DMA's material scope of application also includes number-independent interpersonal communications (i.e., messaging) services, operating systems, web browsers, virtual assistants, and cloud computing services. None of these services are covered by the DSA's material scope of application. That having been said, the DMA may be considered to apply to "intermediary services" in the broadest sense of that notion, in that a CPS shall only be listed in a designation

[33] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, p. 57).

[34] Arts. 29 to 32 DSA.

[35] Art. 1 P2B Regulation.

decision if it constitutes an important gateway for business users to reach end users.[36]

Online advertising services occupy a special position both under the DSA and the DMA. Under the DSA, certain provisions specifically apply to providers of online platforms and of very large services "that present advertisements on their online interfaces."[37] Thus, without taking a position on whether online advertising services constitute a form of intermediary service,[38] the DSA ensures that those services are brought within its material scope of application to a certain degree. Under the DMA, only online advertising services provided by an undertaking that provides another CPS can fall within the DMA's material scope of application.[39] The reason for this restriction was to avoid that providers of purely advertising services would be covered by the DMA, when its objective is to regulate the provision of CPSs (i.e. digital services) in the EU.

These divergent yet intersecting material scopes of application mean that many of the same services that have been designated as "very large" under the DSA have also been listed in the designation decisions of gatekeepers as an important gateway for business users to reach end users under the DMA. That is the case *inter alia* for Google Search, Amazon Store, Apple's App Store, Facebook, Instagram, and TikTok. Conversely, certain services which, at first sight, would qualify for designation under both instruments have not been so designated due to the objectives pursued by the legislation in question.

An example of the latter is X, formerly Twitter, which was designated as a very large online platform in the first batch of designation decisions adopted by the Commission in April 2023,[40] but which the Commission agreed not to designate as a gatekeeper in October 2024, even though it met the quantitative thresholds for such designation. X's user base easily exceeds the 45 million user threshold for designation as a very large online platform under the DSA. That online platform's broad reach means that the societal risks to which it gives rise in relation to the dissemination of illegal and harmful content can be considered systemic in nature and therefore it deserves to be subject

[36] Art. 3(1)(b) DMA.

[37] Arts. 26, 28(2) and 39 DSA.

[38] This is a complicated question, which the CJEU has not yet resolved, given that it touches upon whether the provision of advertising services is truly "neutral" with respect to the advertising content being intermediated. In Joined Cases C-236/08 to C-238/08, *Google France*, EU:C:2010:159, paras. 114 to 120, the CJEU pointed to factors that could be relevant in determining whether the exemption from liability for hosting service providers could apply to Google in relation to its advertising service "AdWords,, but it ultimately reserved the resolution of that question for the national referring court.

[39] Art. 2, point (2)(j) DMA lists as a CPS "online advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by an undertaking that provides any of the CPSs listed in points (a) to (i)."

[40] Commission Decision C(2023)2721 final of 25 April 2023 designating Twitter as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council.

to heightened due diligence obligations. However, the provider of X was able to show that that online social networking service did not constitute an important means for business users to reach end users and that it was therefore not necessary to apply the *ex ante* prohibitions and obligations laid down in the DMA to it,[41] which are meant to ensure fair and contestable markets. The same is true of Microsoft's Bing, which was designated as a very large online search engine under the DSA,[42] but which the Commission decided not to list as an important gateway for business users to reach end users in Microsoft's designation decision,[43] notwithstanding the fact that the presumptions for designation under the DMA were met in relation to that service.

Finally, certain intermediary services exceed the threshold for designation under the DSA, but do not qualify as CPSs under the DMA. An example of this is online platforms hosting pornographic content, four of which have been designated as very large online platforms under the DSA. It is clear why the EU legislature would want to regulate such services under the DSA, but not under the DMA, given the societal harms to which such platforms may give rise, as compared to the lack of a gatekeeper role exercised by such platforms in relation to business users.

### E.2. Personal scopes of application

Although the DSA applies to only one type of digital service, that is, intermediary services, it will apply to a far greater number of providers of such services than the DMA in absolute terms. That is because it imposes a basic set of due diligence obligations on all providers of intermediary services, regardless of their size.[44] Even those DSA obligations that do not apply to micro- and small enterprises will still apply to a larger number of providers than the DMA,[45]

[41] Commission Implementing Decision of 16 October 2024 closing the market investigation opened by Decision C(2024)3117 into X under Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

[42] Commission Decision C(2023)2728 final of 25 April 2023 designating Bing as a very large online search engine in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council.

[43] Commission Implementing Decision C(2024)806 final of 12 February 2024 closing the market investigation opened by Decision C(2023)6078 into Bing, Edge and Microsoft Advertising under Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

[44] Chapter III, Section 1, DSA includes five provisions that apply to all intermediary services providers, while Chapter III, Section 2, DSA includes three provisions that apply to all hosting service providers, including micro- and small enterprises. Section 5, Chapter III, DSA also applies to small- and micro enterprises, provided their service reaches the threshold for designation as a very large online platform or as a very large online search engine laid down in Article 33(1) DSA.

[45] That is the case for the obligations laid down in Section 3, Chapter III, DSA, which apply to online platforms, and the due diligence obligations laid down in Section 4, Chapter III, DSA, which apply to online marketplaces, but which exclude from their scope micro- and small enterprises.

given the latter's high standard for designation as a "gatekeeper," which is a necessary pre-condition for that act to apply to a given provider. The same is true of the most demanding obligations in the DSA for very large online platforms and very large online search engines, since the designation of such services depends solely on their total number of users, whereas the DMA looks at the provider's EU turnover, average market capitalisation, or fair market value and the number of business users using its CPS. In short, while the DMA is likely to apply to a limited number of providers enjoying "gatekeeper" status on the market, the DSA will apply to thousands of small, lesser-known intermediary service providers, as well as to the very large, well-known services often also covered by the DMA.

The addressee of the due diligence obligations laid down in the DSA is the "provider" of intermediary services. The addressee of the obligations and prohibitions laid down in the DMA is the gatekeeper, which that act defines as the "undertaking providing core platform services."[46] While the Commission's proposals for the DSA and the DMA both referred to those addressees as "providers," a conscious decision was taken during the legislative negotiations of the DMA to further specify that notion with the notion of "undertaking" as used in Articles 101 and 102 TFEU. That decision was taken to confirm that the addressees of the prohibitions laid down in EU antitrust law would be the same as the addressees targeted by the obligations and prohibitions in the DMA. In contrast, the scope of the notion of provider used in the DSA was not the focus of legislative negotiations.

This begs the question whether the notion of "provider" used in the DSA has a different scope to the notion of "undertaking providing" used in the DMA. The DSA does not define the notion of "provider." Where that notion is defined in other acts of EU digital law, its definition varies, referring either to a "natural or legal person"[47] or to an "undertaking"[48] providing a service.

There is no compelling reason why the notion of "provider" used in the DSA should differ in meaning from the notion of "undertaking providing" used in the DMA. Whether a particular intermediary service is provided in line with the obligations laid down in the DSA will require decisions to be taken on the

[46] Art. 2(1) DMA.

[47] See e.g. Art. 2(b) e-Commerce Directive which refers to a natural or legal person as the provider and Article 2(2)(a) of Regulation (EU) 2022/612 which refers to an undertaking as the provider. Depending on the scope and objectives of the legal act, that term may also refer to other "bodies,, including Member States or their authorities (Article 4, point 11) of Directive (EU) 2015/2366). Many acts do not define the "provider" (e.g., Directive (EU) 2018/1972 (the European Electronic Communications Code), which instead defines the notion of operator by reference to the notion of "undertaking." See, also, Art 2(3) P2B Regulation, which defines providers of online intermediation services and of online search engines as a natural or legal person. This is curious, since the DMA refers to the definitions of the P2B Regulation to define the notions of online intermediation services and online search engines.

[48] See, e.g., Art. 2(2), point (a), of Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union (OJ L 115, 13.4.2022, p. 1).

presentation and operation of the online interface through which that service is provided.[49] Where an online interface is operated by a subsidiary forming part of a larger corporate group, that technology will often be developed and managed by the parent company of the group and transferred to that subsidiary for the purposes of operating the online interface in the EU. Even if the group uses different online interfaces for the provision of an intermediary service in different Member States, those interfaces will often be based on the same underlying technology, which will normally be developed and managed at the level of the parent company of the group.

Consequently, where an online interface is operated in the EU by a subsidiary forming part of a larger corporate group, ensuring compliance with the obligations laid down by the DSA will generally require strategic decisions to be taken at the level of the parent company of that group in relation to the technology underlying that interface. It is thus the parent company of the group that is able to take the necessary strategic decisions to ensure that the online interfaces operated by its subsidiaries in the EU comply with the obligations laid down in the DSA. A functional approach to the notion of "provider" used in the DSA therefore seems warranted to ensure full compliance with that instrument.

### E.3. Territorial scopes of application

Digital services are unique in that they can be provided to users located in the EU from any other place on earth. The provider of digital services need not have an establishment in the EU to provide those services to users located or established in the EU. The DSA and DMA account for this fact in that they apply to digital services provided to users located or established in the EU, irrespective of where the provider has its place of establishment.[50] This is important given that only a handful of providers of very large services and none of the gatekeepers designated by the Commission are headquartered in the EU. Moreover, while many of those providers have a subsidiary operating the service or an establishment in the EU, not all of them do.

The question that arises in this context is which internet domains must be taken into account when assessing compliance with the DSA and the DMA. The fact that users located in the EU may access the internet domain of a digital service for users in third countries (e.g., the .co.uk or the .com domain) does not necessarily mean that the provider of that domain must also comply with its DSA or DMA obligations in relation to that domain.

[49] As explained in Rec. 70 DSA, the presentation and operation of an online interface lies at the heart of an intermediary service provider's business.

[50] Art. 2(1) DSA and Art. 1(2) DMA. These definitions were already included in Art. 3(4) and (5) TCO Regulation.

The DSA resolves this issue by defining the notion "offering services in the Union" as requiring the provider to have a "substantial connection to the Union."[51] The DSA defines the latter notion as a connection resulting either from an establishment in the EU or from specific factual criteria, such as "a significant number of recipients of the service in one or more Member States in relation to its or their population' or 'the targeting of activities towards one or more Member States."[52] An example of the former could be a significant number of recipients located in Ireland that make use of the service's .co.uk website. An example of the latter could be a third country provider that targets EU residents by offering services in multiple EU languages, offering payment for goods or services in Euros, or offering shipping to the EU.[53] The mere fact that a website is accessible to EU residents does not constitute on its own a substantial connection to the EU.[54]

For its part, the DMA does not regulate this issue beyond providing that that act applies to CPSs provided by gatekeepers to users in the EU irrespective of where those gatekeepers are established and irrespective of the law otherwise applicable to the provision of the service. Further regulation is probably not needed, as the DMA only applies to gatekeepers, which are generally large multinationals with an establishment in the EU. By contrast, the DSA applies to all intermediary services provided to users located in the EU, irrespective of their size or number of users.[55] Notwithstanding this difference, it still begs the question to which internet domains the provisions of the DMA apply. To achieve the objectives of that instrument, its prohibitions and obligations should apply to those domains that business users use to reach end users located in the EU. That could mean that a co.uk or a .com domain could be caught by the provisions of the DMA.

Of course, none of these solutions resolve the tricky issue of supervising and enforcing the DSA and the DMA in relation to entities located wholly outside the EU. That issue has already arisen in the context of antitrust enforcement, where the lack of extra-territoriality means that fines cannot be enforced against undertakings established entirely outside the EU. The DSA attempts to resolve that issue by requiring providers of intermediary services established outside the EU to appoint a legal representative inside the EU.[56] The DSA further provides that those representatives may be held liable for non-compliance of DSA obligations by the provider.[57] This is without prejudice to the liability and legal actions that may be initiated against the provider itself.

---

[51] Art. 3(d) DSA.

[52] Art. 3(e) DSA.

[53] Rec. 8 DSA.

[54] Ibidem.

[55] Certain DSA due diligence obligations do not apply to micro- and small enterprises. See n. 45 above.

[56] Art. 13(1) DSA.

[57] Art. 13(3) DSA.

Taken literally, this would mean that fines could be collected from the legal representative. In this regard, the DSA requires the provider to mandate its legal representative for the purpose of being addressed on all issues necessary for compliance with and enforcement of decisions and to provide its legal representative with necessary powers and sufficient resources to comply with such decisions.[58] It is to be seen how difficult this will make appointing a legal representative in the EU. In the end, if such a representative has insufficient resources to comply with a decision adopted under the DSA, the Commission or Digital Service Coordinator, that is, the national authority competent for supervising and enforcing the DSA at Member State level, will have to attempt enforcement against an entity established outside the EU with all the pitfalls that that entails.

### F. Diverging yet intersecting supervision and enforcement frameworks

Whereas the DMA is exclusively supervised and enforced by the Commission, the DSA foresees complementary supervisory and enforcement tasks for the Commission and the Digital Service Coordinators depending on the size of the service and the obligations at stake. As explained in the subsequent chapters, this centralised supervision and enforcement of those instruments by the Commission makes those pieces of digital services legislation unique as compared to other pieces of digital services legislation. For example, the AVMSD,[59] the P2B Regulation, and the TCO Regulation[60] all place supervision and enforcement solely in the hands of national competent authorities, as does the GDPR,[61] whose concepts are of particular relevance in relation to numerous obligations and prohibitions laid down in the DSA and the DMA which make a direct reference to those concepts. Being regulations, which "have general application" and are "binding in [their] entirety and directly applicable in all Member States,"[62] the DSA and the DMA may also be privately enforced in the courts of the Member States.

When it comes to the supervision and enforcement of the DSA and the DMA by the Commission, the first thing that strikes a reader comparing those two acts in relation to that matter is the similarity of their provisions. The second

[58] Art. 13(2) DSA.

[59] 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) (OJ L 95, 15.4.2010, p. 1).

[60] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (OJ L 172, 17.5.2021, p. 79).

[61] 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 (OJ L 119, 4.5.2016, p. 1).

[62] Art. 288 TFEU.

thing that strikes a reader is the similarity of those provisions to the provisions on supervision and enforcement of Article 101 and 102 TFEU by the Commission as enshrined in Regulation 1/2003.[63] That similarity is unsurprising, as it was considered better to have recourse to a tried and tested system of supervision and enforcement by the Commission, rather than to reinvent the wheel. Nevertheless, certain differences exist between similar provisions in the DSA and the DMA, as well as between similar provisions in the DSA and the DMA, on one hand, and Regulation 1/2003, on the other.

Already at the outset, the DSA empowers the Commission to deploy its investigatory powers only "[f]or the purposes of investigating compliance of providers of very large online platforms and of very large online search engines with the obligations laid down in this Regulation."[64] Its investigatory powers are then further curtailed by specifying that they may only be deployed "[i]n order to carry out the tasks assigned to it under [Section 4 of Chapter IV]."[65] By contrast, the DMA and Regulation 1/2003 allow the Commission to deploy such powers "[i]n order to carry out its duties under this Regulation."[66]

This may seem like a trivial difference, but it has concrete consequences for the Commission's decision-making practice. For example, prior to the designation of a service as a very large online platform or very large online search engine, the Commission is only empowered to request additional information from the provider on the calculation it performed to determine the average monthly active recipients of its service in the EU, including explanations and substantiations of the data used,[67] and not, for example, on the corporate structure of the provider, since it has no general competence to request information from providers whose services have not been designated as very large. The reason for this difference probably lies in the fact that the DMA was always intended to be monitored and enforced solely by the Commission, while the DSA's supervision and enforcement mechanism was altered during the legislative negotiations as a result of which the Commission was given primary responsibility for designation, supervision and enforcement of very large online platforms and very large online search engines.

Even where the DSA does allow the Commission to deploy its investigatory powers, it appears to place a higher standard of motivation on their deployment than under the DMA or Regulation 1/2003. For example, the DSA provision empowering the Commission to request information explicitly refers to "information relating to the suspected infringement" as justifying recourse to that investigatory power. This explains why the Commission is not entitled to request information on the corporate structure of the provider in the proceed-

[63] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (OJ L 1, 4.1.2003, p. 1).

[64] Art. 65(1) DMA.

[65] Arts. 67(1), 68(1) and 69(1) DSA.

[66] Arts. 21(1), 22(1), and 23(1) DMA; Arts. 18(1), 19(1), 20(1) Regulation 1/2003.

[67] Art. 24(3) DSA.

ings leading up to the adoption of its supervisory fee decisions,[68] since at that stage there is no suspicion of an infringement justifying recourse to a request for information. By contrast, the DMA provision empowering the Commission to request information simply refers to "all necessary information,"[69] as does the similar provision in Regulation 1/2003.[70] The same difference emerges as regards the power to take interviews and statements, but curiously not for the power to conduct inspections, which is similarly worded across all three instruments.

Otherwise, certain of the Commission's enforcement powers are phrased differently in the DSA and the DMA without it being clear whether that difference has an impact on the exercise of those powers. For example, the DSA does not list the imposition of interim measures as a decision requiring the adoption of preliminary findings.[71] By contrast, the DMA does require such a prior administrative step,[72] as does Regulation 1/2003.[73] Conversely, neither the DMA nor Regulation 1/2003 requires the adoption of preliminary findings prior to imposing periodic penalty payments, but only where the definitive amount is set following compliance with the obligation that the periodic penalty payment was intended to enforce.[74] The DSA does not make any similar distinction,[75] although that appears to be the result of an oversight, since it is unclear how the Commission could adopt effective periodic penalty payments to ensure rapid compliance with obligations under the DSA if it is required to first solicit the views of the provider on those penalties.

As regards differences with Regulation 1/2003, the DSA and the DMA contain a novel supervisory mechanism which empowers the Commission to take "the necessary actions to monitor the effective implementation and compliance with this Regulation."[76] The provisions in question list certain examples of what such a mechanism might entail, including requiring the provider to retain all documents deemed to be necessary to assess the implementation of and compliance with the obligations of that act and appointing independent external experts and auditors, as well as experts and auditors from competent national authorities with the agreement of the authority concerned, to assist the Commission in supervising the effective implementation and compliance with the relevant provisions of those acts and to provide specific expertise or knowledge to the Commission. While the DSA lists requiring the provider to

[68] The Supervisory Fee Delegated Regulation only refers to information requested pursuant to Article 24(3) DSA, thus information on the calculation used to estimate a service's average monthly active recipients.

[69] Art. 21(1) DMA.

[70] Art. 18(1) Regulation 1/2003.

[71] Art. 79(1) DSA which does not refer to Art. 70 DSA.

[72] Art. 34(1) DMA which refers to Art. 24 DMA.

[73] Art. 27(1) Regulation 1/2003 which refers to Art. 8 of that regulation.

[74] Art. 34(1) DMA only refers to Art. 31(2) DMA.

[75] Art. 79(1) DSA refers to Art. 74 DSA as a whole.

[76] Art. 72 DSA and Art. 26 DMA.

grant access to, and explanations relating to, its databases and algorithms as an example one such monitoring mechanism, the DMA includes as part of the Commission's competence to request information.[77] That difference may be explained by the fact that the Commission may not request information under the DSA until it suspects an infringement. In any event, these are just examples, making the broad wording of the monitoring mechanisms in the DSA and DMA potentially limitless. It is clear that the Commission should not be able to circumvent the procedural safeguards in other provisions of the DSA and the DMA,[78] but beyond that restriction, the limits of the Commission's broad supervisory power are unclear and will have to be tested over time. Another important difference between the DSA and the DMA, on the one hand, and Regulation 1/2003, on the other, is the access to documents procedure. Not only do the former not foresee the role for a hearing officer; they also limit the documents to which providers of digital services may obtain access during non-compliance procedures. While non-confidential versions of all documents cited in the preliminary findings are directly shared with the provider, other information from the Commission's case file, such as documents not cited in the preliminary findings and confidential documents, are only shared with specified external legal and economic counsel and technical experts, which are not in an employment relationship with the providers, under a "confidentiality rings" procedure. This is meant to ensure maximum access, while protecting third-party rights and fulfilling the Commission's obligation to protect confidential information.

## G. Complementary regimes

The Digital Services Package was not adopted in a regulatory vacuum. Both prior to and since the adoption of the DSA and the DMA, the EU legislature adopted several acts of more limited application regulating the provision of digital services in the EU. The Draghi report refers to "around 100 tech-focused laws" regulating the provision of digital services in the EU, but that is an exaggeration.[79]

[77] Art. 21(1) DMA.

[78] E.g., the Commission should be able to rely on its general supervisory power to send requests for information where the conditions of Art. 67 DSA or Art. 21 DMA are not met, nor should it be able to request access to data where the conditions of Art. 40 DSA are not met.

[79] See Draghi Report, p. 30. In support of the claim that "the EU's regulatory stance towards tech companies hampers innovation," the report cites the Breugel Foundation's 2024 EU Digital Policy Overview, but most of the laws listed there do not directly regulate the provision of digital services in the EU. They are either meant to promote technology in the EU (i.e., the Digital Europe Programme Regulation, the Recovery and Resilience Facility Regulation, the EuroHPC Regulation, the Chips Act, etc.) or they apply to a particular digital service as an incidental consequence of that service falling within the scope of application of the legislation in question (i.e., the Product Liability Directive, the Unfair Contract Terms Directive, the Toys Regulation, the Law Enforcement Directive, Administrative Cooperation in the Field of taxation, the Common VAT system, etc.).

In reality, the AVMSD, the Copyright in the Digital Single Market Directive ("Copyright in the DSM Directive"),[80] the P2B Regulation, and the TCO Regulation are examples of EU legislative acts that addressed in a more targeted manner several of the societal and competitive harms that the DSA and the DMA were designed to address comprehensively. Since the adoption of the DSA and the DMA, the EU legislature has enacted a handful of legislative acts that also regulate certain specific aspects of the provision of digital services in the EU, in some cases going beyond the provisions of the DSA and the DMA: the Political Advertising ("Pol Ads") Regulation,[81] the European Media Freedom Act (EMFA)[82] and the General Product Safety Regulation (GPSR)[83] all include dedicated provisions on the provision of certain type of digital services. The question arises how all these legislative acts are to be applied concurrently.

As regards the DSA in particular, it provides that it 'is without prejudice to the rules laid down by other Union legal acts regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing this Regulation" and subsequently lists as examples all the aforementioned acts adopted prior to its adoption. The DMA contains no similar provision.

A distinction is thus made in the DSA between "rules regulating other aspects of the provision of intermediary services" and rules "specifying and complementing" the DSA. What is meant by the first category of rules is relatively straightforward: it concerns rules governing intermediary services on matters falling outside the scope of the DSA. Although, remarkably, not expressly mentioned, the DMA is an example of such rules. Other examples include EU competition law, labour law, and data protection law, to name a few. The more complex question is when rules may be considered as "specifying and complementing" the DSA and what is the consequence of either qualification for the relationship between the DSA and those rules.

For example, under the AVMSD, which was amended in 2018 to include provisions regulating video-sharing platforms, Member States must ensure that providers of such platforms adopt appropriate measures to protect minors from harmful content.[84] That rule would appear to constitute a specification

[80] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, p. 92)

[81] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (OJ L, 2024/900, 20.3.2024).

[82] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act) (OJ L, 2024/1083, 17.4.2024).

[83] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (OJ L 135, 23.5.2023, p. 1).

[84] Art. 28b(1) AVMSD.

of the rules in the DSA that online platforms that are accessible to minors must put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors.[85] But what of the rule in the AVMSD requiring Member States to ensure that video sharing platform providers adopt appropriate measures to protect all users from content containing incitement to violence or hatred and from content the dissemination of which constitutes an activity which is a criminal offence under EU law? Do the mechanisms that the DSA require intermediary service providers to adopt constitute such measures? An interesting follow-up question is to what extent a Member State may continue to impose on video-sharing platform providers measures that are more detailed or stricter measures. While the AVMSD expressly allows for this possibility,[86] doing so could undermine the exhaustive harmonisation to which the DSA strives and would therefore be impermissible. A case-by-case assessment would therefore be necessary and may need to be conducted by the Commission under the mechanism provided for in Directive 2015/1535.

Another interesting question is how to treat EU legislation where it is only more specific in relation to certain aspects covered by the DSA. For example, the Copyright in the DSM Directive, which regulates "online content-sharing services," contains a provision further specifying how the liability exemption for hosting service providers, previously laid down in the e-Commerce Directive and now laid down in the DSA, should apply to such services.[87] Another question is whether the mechanisms laid down in the Copyright in the DSM Directive to ensure transparency, sufficiently substantiated notices, and the rules on misuse constitute "specifications" in relation to the DSA. The answer to that question will depend on the exact circumstances of each case and require a balancing of the different sets of applicable provisions. The same is true for the TCO Regulation, which contains more detailed requirements than the DSA on transparency, removal orders and due diligence measures, including notice and action, for online platform providers exposed to terrorist content.

As regards EU legislation regulating the provision of digital services adopted after the adoption of the DSA, it contains a mix of specifying and complementary provisions. For example, the GPSR contains a provision on online marketplaces that both specifies obligations already contained in Chapter III,

[85] Art. 28(1) DSA.

[86] Art. 28b(6) AVMSD.

[87] Art. 17(3) and (4) Copyright in the DSM Directive: the provider must obtain an authorisation from the rightsholder, failing which it must demonstrates that it has made best efforts to obtain such an authorisation, that it has made best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information, and, in any event, that it has acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholder, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads.

Section 4, of the DSA and complements those obligations with cooperation and transparency obligations in line with its product safety rationale.[88] Similarly, the Pol Ads Regulation, which applies to all forms of political advertising including online advertisements, supplements the transparency and due diligence obligations applicable to intermediary service providers that publish advertisements on their online interfaces.[89] The same is true for the EMFA, which imposes additional obligations on providers of very large online platforms designated under the DSA.[90]

Of all the complementary regimes mentioned, the P2B Regulation is unique in its relationship to the DSA and the DMA, since it displays features akin to both instruments. It already addresses issues of transparency in relation to the terms and conditions of providers of online intermediation services and online search engines in favour of business users,[91] which are further elaborated upon for all providers of intermediary services in relation to all users under the DSA.[92] It also addresses the modalities of restriction, suspension, and termination of service by providers of online intermediation services and online search engines in relation to business users,[93] which are further elaborated upon for all hosting service providers in relation to all users under the DSA.[94] Finally, it requires providers of online intermediation services and online search engines to set out in their terms and conditions the main parameters determining ranking and the reasons for the relative importance of those main parameters as opposed to other parameters,[95] while providers of online intermediation services are to set out in their terms and conditions any restrictions on the ability of business users to offer the same goods and services to consumers under different conditions through other means than

[88] E.g., Art. 22 GPSR

[89] The obligation that will have the most prominent visible impact for users of intermediary services is the one to label political advertisements as such (Art. 11 Pol Ads Regulation). In addition, the Pol Ads Regulation supplements the type of information that the DSA obliges providers of very large online platforms and very large online search engines to include in their advertisement repository (Arts. 13(2) and 12(1) Pol Ads Regulation and Art. 39 DSA). Finally, the Political Advertisement Regulation initially took a stricter approach to regulating the use of targeting and ad-delivery techniques that involve the processing of personal data in the context of online political advertising, but such practices were subsequently banned under the DSA at the instigation of the European Parliament (Art. 26(3) DSA), leaving limited scope for the application of the provision on such techniques to circumstances in which no service is provided (Arts. 18-20 Pol Ads Regulation).

[90] In particular, such providers must provide a functionality to their users to declare that they are media service providers and that they comply with certain transparency requirements (Art. 18(1)-(3) EMFA). EMFA further requires such providers to provide a statement of reasons to media service providers before suspending its service to them or restricting the visibility of their content due to a breach with their terms and conditions and to give those providers the opportunity to respond within 24 hours before any such action is undertaken (Art. 18(4) EMFA).

[91] Art. 3 P2B Regulation.

[92] Art. 14 DSA.

[93] Art. 4 P2B Regulation.

[94] Art. 17 DSA.

[95] Art. 5 P2B Regulation.

through those services.[96] The DSA imposes a similar transparency obligation as regards all recommender systems on all providers of online platforms,[97] while the DMA prohibits gatekeepers from imposing such restrictions.[98] Finally, the DMA draws on the P2B Regulation for several of its definitions, which means that the material scope of the former will depend on a determination of the latter.[99] The biggest deficiency in relation to the P2B Regulation to date has been a general lack of awareness of its existence and a rather weak and open-ended enforcement mechanism which it places entirely in the hands of Member State authorities.[100]

Providers of digital services covered by the DSA and the DMA may also have to consider the application of the Artificial Intelligence (AI) Act[101] where they incorporate AI into their services. A pertinent example of a digital service increasingly reliant on AI is online search engines, while recommender and other algorithmic systems used by other digital service providers are increasingly based on AI. The provisions of the AI Act are most likely to apply concurrently with those of the DSA on content moderation, dark patterns and recommender systems. However, for that to be the case, the AI system in question must in some way be involved in the provision of intermediary services, since only the latter fall within the material scope of application of the DSA. Where the AI system itself is the service offered by the provider, only the provisions of the AI Act will apply to that system. Moreover, while the rules of the AI Act are likely to apply to the system as such (i.e., its development and use), the DSA will regulate how the dissemination of the illegal or harmful content is amplified through the recommender system in the user interface or how the dark patterns deceive users of that interface. As regards the DMA, AI systems are not themselves listed as a CPS, so they will only be covered by the prohibitions and obligations of the DMA where they form part of such a service.

All these complementary regimes regulating the provision of digital services in the EU raises the question whether the lack of regulation in the two decades prior to 2019 mentioned in Section B above has given way to the overregulation of such services in the past five years. The DSA and DMA are horizontal legal instruments precisely meant to prevent excessive regulation of digital services by limiting the number of addressees on whom the most demanding

[96] Art. 10 P2B Regulation.

[97] Art. 27 DSA (with the exception of micro- and small enterprises).

[98] Art. 5(3), (4) and (5) DMA.

[99] But not the personal scope, since the P2B Regulation applies to "providers" which it defines as "natural and legal persons," not "undertakings."

[100] Art. 15 P2B Regulation.

[101] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024)

obligations are placed. However, digital services are currently in vogue, thus any opportunity to revise existing legislation or devise new legislation for the digital age gives rise to the temptation to include provisions specifically addressed to providers of such services regardless of the area being regulated.[102] Excessive complementary legislation on digital services could undermine the Digital Services Package's objective of facilitating innovation in those services. While very large digital service providers typically have the financial and technical resources to comply with their obligations under these numerous regimes, not all complementary regimes referred to above apply a graduated approach to regulation, nor do they always exclude micro- and small digital service providers from their remit.

At the end of the day, the DSA and the DMA, if thoroughly implemented and enforced, will have a profound impact on the provision of digital services in the EU. What the DSA and the DMA ultimately have in common is their aim to regulate services which have come to form an important part of the lives of EU citizens and businesses. Abandoning a *laissez-faire* and *ex post* approach to regulation, the rules by which digital services may be provided in the EU are now set out clearly in advance in those two acts, increasing legal certainty and predictability of outcomes by preventing a plethora of national rules seeking to address the same societal and competitive harms. Only time will tell whether the DSA and the DMA will achieve the lofty goals that the EU legislature has set out for those instruments.

## PART II: DIGITAL SERVICES ACT (DSA)

### A. Introduction

In the first case on the DSA to reach the Court of Justice, its Vice-President described this novel piece of legislation as "a central element of the policy developed by the EU legislature in the digital sector," which "pursues objectives of great importance."[103] This view of the DSA's importance is broadly shared in the legal literature.[104] Recent events relating to topics covered by the DSA have

[102] See, e.g., Regulation (EU) 2023/1542 of the European Parliament and of the Council concerning batteries and waste batteries and Regulation (EU) 2025/40 of the European Parliament and of the Council of 19 December 2024 on packaging and packaging waste, which include provisions on online marketplaces mirroring provisions in Arts. 30 and 31 DSA.

[103] Order Vice-President Court of Justice, Case C-639/23 P(R), *Commission v. Amazon*, EU:C:2024:277, para. 155.

[104] E.g., A. Savin, 'The EU Digital Services Act: Towards a more responsible internet,' *Copenhagen Business School CBS LAW Research Paper* No. 21-04, 2021, p. 14 (referring to the DSA proposal as being "among the most important documents in digital regulation"); M. Eifert, A. Metzger, H. Schweitzer and G. Wagner, 'Taming the giants: the DMS/DSA package,' *Common Market Law Review* 58 2021, pp. 987-1028, at p. 994 (calling the DSA (and DMA) "a turning point in European

shown its relevance in practice. Think, for instance, of the arrest of the CEO of messaging service Telegram,[105] the debates surrounding the functioning of microblogging service X (formerly Twitter),[106] or the impact that social media platform TikTok was deemed to have had on the presidential elections in Romania.[107] One could say that the DSA's importance corresponds to the importance of the internet in general and the digital services covered in particular for all kinds of political, commercial, cultural, and entertainment purposes and thus, in essence, for virtually all aspects of modern-day life. Indeed, the DSA is to a large extent driven by the view that especially certain large digital services have become "de facto public spaces,"[108] which as such require proper regulation.

The fact that its importance is beyond doubt does not mean, however, that the DSA is necessarily easily understood or straightforward to apply. In the relatively limited time that it has been applicable, not only the promise of, but also certain potential challenges relating to the approach it embodies have become apparent. Against this background, and building on the general discussion in Part I of this report, the present Part II seeks to highlight a number of key issues and to take stock of the main experiences gathered with the DSA thus far.[109] To that aim, first a number of general comments are made.[110] These center on what are arguably the DSA's central concepts, namely, diligence, balance, and evolution. Subsequently, attention turns to the initial experiences gained with the exercise of the Commission's tasks under the DSA as implementor, designator, and supervisor. Finally, certain specific topics are discussed relating to the DSA's application in practice.[111]

---

platform regulation"); D. Keller, 'The EU's new Digital Services Act and the rest of the world', in: J. van Hoboken et all (eds.), *Putting the DSA into practice*, Verfassungsbooks 2022, pp. 227-241, at p. 229 (speaking of "a major milestone in the history of platform regulation").

[105] E.g., 'Telegram CEO Pavel Durov arrested at French airport,' *BBC News*, 25 August 2024.

[106] E.g., 'Musk's X banned in Brazil after disinformation row,' *BBC News*, 31 August 2024; 'Elon Musk launches profane attack on X advertisers,' *BBC News*, 30 November 2023.

[107] E.g., 'Romanian court annuls result of presidential election first round,' *BBC News*, 6 December 2004.

[108] Commission, Impact assessment DSA (part 1/2), SWD(2020) 348, 15 December 2020, p. 9.

[109] For a more general overview of the DSA, see F. Wilman, 'The Digital Services Act (DSA): an overview,' 2022, available via https://ssrn.com/abstract=4304586

[110] See also F. Wilman, 'Conclusion,' in: F. Wilman, S. Kalėda and P.J. Loewenthal, *The EU Digital Services Act: a commentary*, OUP 2024, pp. 522–531 (containing more extensive general comments on the DSA).

[111] These topics reflect as much as possible those highlighted in the FIDE questionnaire prepared for the national rapporteurs, whilst bearing in mind however the specificities of the institutional perspective taken in this Report.

## B. General comments

### B.1. Diligence

As set out in Part I, the DSA applies to intermediary services.[112] In essence, these are services involving the transmission and storage of information provided by third parties (in other words, user-generated content). The DSA regulates these services in a layered manner. Broadly speaking, the more actively involved the service provider is – in particular in terms of not only storing but also disseminating third-party information to the public, thus making it an "online platform"[113] – and the larger the scale at which the service is operated – in particular if it exceeds the threshold of 45 million average monthly active users[114] in the EU that the DSA sets for qualifying it as "very large"[115] – the more far-going the obligations are that the DSA imposes in respect of the service in question.

On the substance, the central concept of the DSA's obligations is that of due diligence. The DSA translates this concept essentially into two distinct types of obligations. For the first type, the due diligence involves efforts aimed at tackling illegal content, subject to certain safeguards. Thus, the primary "danger" to be addressed in these cases is external to the service provider and consists of users providing illegal content. The activities to be undertaken are repressive in nature and should be as effective as reasonably possible.[116] At the same time, it is acknowledged that there is a related, secondary "danger," namely, that of the repressive activities overshooting. Such overshooting could take various forms, such as wrongly removing information that is not actually illegal content, excessively monitoring users' behavior or processing their personal data, or using technical means that are not accurate and up to date.

Under the DSA this kind of content-focused, "repressive diligence" is at play, for instance, where service providers: process notices of illegal content submitted by third parties through the mandatory notice and action mechanisms, including where those notices originate from parties that are deemed to have particular expertise, such as NGOs dedicated to combating matters like child sexual abuse material or hate speech (so-called "trusted flaggers");[117] act voluntarily to tackle illegal content under the DSA's "Good Samaritan" clause;[118] or take the required measures to combat misuse of its service consisting of users frequently providing manifestly illegal content.[119] The DSA's prohibition of

[112] Art. 3(g) DSA.

[113] Art. 3(i) DSA.

[114] The DSA speaks of "recipients of the service" rather than "users." As the latter is the shorter and more commonly used term, that term is used in this contribution.

[115] Art. 33 DSA.

[116] Cf. Case C-314/12, *UPC Telekabel Wien*, EU:C:2014:192, para. 62.

[117] Arts. 16 and 22 DSA.

[118] Art. 7 DSA.

[119] Art. 23 DSA.

imposing general monitoring obligations on intermediary service providers[120] and the latter's obligation to provide transparency *ex post* on the measures taken[121] act in this connection as a sort of horizontal safeguarThe second kind of due diligence requirements is different. True, the "danger" at issue still manifests itself in connection to third-party information, as is by definition the case under the DSA. Yet the primary concern is not so much *what* the service providers intermediate, but rather *how* they do so. In other words, the focus is not on repressing illegal content and the associated risk of overshooting, but rather on the service providers' own activities in providing the service. Here the concept of due diligence is elaborated into self-standing obligations or prohibitions imposed on intermediary service providers. The main aim is to protect users against negligent, manipulative, arbitrary, or excessive practices on the part of those service providers.

Examples of such service-focused, "protective diligence" requirements of the DSA include: the obligation for service providers to give clarity upfront about the applicable terms and conditions and to respect limits in the way that these are enforced;[122] the ban on manipulative behavior in connection to the design and organization of service providers' online interfaces (that is, their websites or apps), known as "dark patterns";[123] the transparency required and the limits set in connection to advertising;[124] the transparency and user agency requirements in respect of recommender systems;[125] and the required protection of minors.[126] Under the DSA's layered approach, very large service providers[127] are subject to additional obligations, most notably to conduct an annual risk assessment and mitigation exercise.[128] Whilst somewhat harder to categorize, these are also best seen as due diligence requirements of this second type.[129]

The former, "repressive diligence"-type of requirements are in essence manifestations of the duty of care already recognised by the e-Commerce Directive, which dates from 2000 and which, as explained in Part I, can be seen as the DSA's predecessor. Especially in the case of hosting services, the conditions attached to the liability exemptions contained in that Directive, which have since

[120] Art. 8 DSA.

[121] Arts. 15 and 24 DSA.

[122] Art. 14 DSA.

[123] Art. 25 DSA.

[124] Arts. 26 and 39 DSA.

[125] Arts. 27 and 38 DSA

[126] Art. 28 DSA.

[127] That is, very large online platforms and very large online search engines, which have been designed as such in accordance with Art. 33 DSA.

[128] Chapter III, Section 5, DSA.

[129] E.g., whilst the risk assessment and mitigation obligations of Arts. 34 and 35 DSA also relate to systemic risks consisting of the dissemination of illegal content, that is only one of four categories of such systemic risks. Moreover, the overall focus of the risk assessment and mitigation is on the contribution of the service in question (in terms of its design, functioning and use) to those systemic risks.

been transferred to the DSA,[130] were designed to encourage service providers to act diligently in respect of illegal content that they may encounter.[131] What is more, under the Directive Member States had the possibility to add "duties of care […] in order to detect and prevent certain types of illegal activities."[132] The DSA now essentially articulates such duties of care in a harmonized manner at EU level, including the safeguards deemed necessary.

Although under the DSA users are not necessarily consumers, the requirements of the second, "protective diligence"-type are more consumer protection-like in appearance. They tend to focus on service providers' core activities, like using recommender systems to bring information to users' attention, advertising, and data-related practices. The DSA's provisions in question can accordingly resemble or even overlap with, and sometimes also rely on concepts from, EU consumer protection law and the General Data Protection Regulation (GDPR).[133] Nonetheless, the DSA should not be seen as a consumer or data protection instrument properly speaking. The context and underlying aim of the obligations are different. As noted earlier, the regulated services essentially involve the intermediation of third-party speech. The focus is therefore on addressing speech-related harms, particularly those negatively affecting the exercise of the freedom of expression and information as well as other fundamental rights, connected to the service provision, such as the unjustified removal of legal content, the creation of unwanted filter bubbles, practices harmful to minors, and election manipulation.

### B. 2. Balance

Ultimately, the DSA naturally aims to address both types of challenges mentioned above, that is, those resulting from third-party information as such, as well as those resulting from the service providers' own activities when intermediating the information. According to its Article 1(1), the DSA seeks to ensure that the online environment is not only *safe*, but also *predictable* and *trusted*.

---

[130] Arts. 4, 5 and 6 DSA (formerly Art. 12-14 e-Commerce Directive). See also Art. 89 DSA (deleting those articles from the e-Commerce Directive). See further, e.g., Opinion AG Szpunar Case C-492/23, *Russmedia*, EU:C:2025:68, paras. 42-96 (discussing the liability exemption for hosting).

[131] Cf. Case C-324/09, *L'Oréal v. eBay*, EU:C:2011:474, paras. 120-124; C-682/18 and C-683/18, *YouTube and Cyando*, para. 115 (both using as a standard that of a diligent operator). See also Art. 17(4) Copyright in the DSM Directive, which expressly requires professional diligence.

[132] Rec. 48 e-Commerce Directive.

[133] 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) (OJ L 119, 4.5.2016, p. 1). See, e.g., Art. 25(2) DSA (seeking to avoid overlaps with EU consumer protection law and the GDPR in connection to the regulation of "dark patters") and Art. 26(3) DSA (relying on the GDPR concepts of "profiling" and "special categories" of personal data in connection to the DSA's regulation of advertising).

Article 1(1) DSA also refers to the aim of effectively protecting the fundamental rights. It is noticeable that the reference is to the fundamental rights enshrined in the Charter of Fundamental Rights of the EU ("the Charter") in general. That indicates that the DSA does not aim to "implement" one or several specific fundamental rights. That sets it apart from, for instance, the GDPR or the EU copyright acquis. It will be interesting to see what this means for the manner in which the DSA is interpreted, bearing in mind that the Court of Justice of the EU (CJEU) tends to consider the aims pursued by a given act of EU law a particularly important interpretative element. Indeed, such teleological interpretation has been key to the expansive way in which the GDPR and the copyright acquis have often been interpreted.[134] Arguably, Article 1(1) DSA should be read as stating that, first and foremost, the DSA aims to achieve a *balance* between the various fundamental rights typically at stake in disputes arising under it. Thus, it could be said that rather than "implementing" one or the other specific fundamental right, the DSA seeks to give effect to CJEU's case law insisting that in such cases of conflicting fundamental rights a "fair balance," in accordance with the principle of proportionality, must be struck.[135] The aforementioned distinction between the due diligence provisions of the DSA with a "repressive" and a "protective" character can be of relevance in this regard. Where provisions of the former type are at stake, a three-way balance is typically called for.[136] First of all, the freedom of expression and information tends to be at issue.[137] This fundamental right is relevant both for the users who provided the information that might be repressed for being illegal content and for the users who might wish to access that information. The importance of the internet and digital services for free expression and obtaining information, as often emphasized by the CJEU,[138] makes that this is a particularly important fundamental right in the present context. However, it is certainly not the only – or even necessarily the predominant – one. Account should also be taken of the fundamental rights of the persons aggrieved by illegal content, such as the right to protection of intellectual property of a party whose copyright has been infringed, or the right to a private and family life of persons whose honour or

[134] E.g., C-487/21, *F.F. v Österreichische Datenschutzbehörde*, EU:C:2023:369, para. 40 (concerning the GDPR); Case C-607/11, *TVCatchup*, EU:C:2013:147, para. 20 (concerning copyright).

[135] E.g., Case C-275/06, *Promusicae*, ECLI:EU:C:2008:54, para. 68.

[136] E.g., C-682/18 and C-683/18, *YouTube and Cyando*, para. 113; Case C-70/10, *Scarlet Extended v. SABAM*, EU:C:2011:771, paras. 44-53.

[137] Art. 11 Charter.

[138] Case C-401/19, *Poland v. EP and Council*, EU:C:2022:297, para. 46 (stating that the internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, that online content-sharing platforms play an important role in enhancing the public's access to news and facilitating the dissemination of information in general and that user-generated expressive activity on the internet provides an unprecedented platform for the exercise of freedom of expression). The same goes for the European Court of Human Rights (ECtHR); see, e.g., ECtHR *Sanchez v. France*, Appl. no. 45581/15, paras. 158-162 (noting also certain risks connected to the internet).

privacy has been violated.[139] Their right to an effective judicial remedy can also play a role.[140] Finally, the service providers themselves have fundamental rights too, notably their freedom to conduct a business.[141]

Where DSA provisions of the latter, "protective" type are at stake, things may play out somewhat differently. The relationship may not always be triangular in nature, yet the required balancing can still be complex. Think, for instance, of the question how the service providers' freedom of contract, as part of the freedom to conduct a business, can be squared with users' freedom of expression when it comes to the content, application, and enforcement of contractual restrictions imposed by the former. That question is particularly relevant considering that some of the services covered are of great importance for reaching a public and that, in practice, most content moderation takes place based on the terms and conditions rather than the law as such. That being so, the DSA contains a provision expressly requiring service providers to have due regard to users' fundamental rights in this connection.[142] Other relevant questions include how decisions to demote or not recommend certain third-party information (rather than simply removing it) are to be assessed from the angle of freedom of expression and information;[143] how the fundamental rights of advertisers are to be factored in under the DSA's advertising-related provisions;[144] and how the rights of the child play out when seeking to protect minors.[145] The fact that Article 1(1) DSA makes express reference to the principle of consumer protection could be of particular interest when interpreting and applying DSA provisions of this "protective" type.[146]

As a final point it is worth noting that Article 1(1) DSA refers also to facilitating innovation. This point connects to debates about possible overregulation, already touched upon above.[147] One the one hand, through its layered design and differentiation based on the nature and the size of the services,[148] the DSA

[139] Arts. 17 and 7 Charter, respectively.

[140] Art. 47 Charter.

[141] Art. 16 Charter. In addition, service providers' own freedom of expression could conceivably come into play. The latter element has to date not featured in the relevant CJEU case law, but it has in that of the ECtHR. See, e.g., ECtHR *Delfi v. Estonia*, Appl. no. 64569/09.

[142] Art. 14(4) DSA. See further, e.g., J.P. Quintais, N. Appelman and R. Ó Fathaigh, 'Using Terms and Conditions to apply Fundamental Rights to Content Moderation,' *German Law Journal* 24 2023, pp. 881–911.

[143] As no information is being removed, it remains accessible. However, given the typically enormous amounts of information stored and disseminated to the public, the question could arise whether such accessibility is not merely theoretical.

[144] In particular, Arts. 26 and 39 DSA. See, e.g., C-639/23 P(R), *Commission v. Amazon*, para. 131.

[145] Art. 24 Charter.

[146] Art. 38 Charter.

[147] See Part I, Section G, above. See further, e.g., A. Bradford, 'The false choice between digital regulation and innovation,' *Northwestern University Law Review* 2024 119, pp. 377–453.

[148] Such size-based differentiation occurs in two ways. First, as described above, specific obligations apply to designated very large services (Chapter III, Section 5). Second, the DSA contains several exemptions for small and micro enterprises (Arts. 15(2), 19 and 29).

clearly seeks to avoid imposing excessive regulatory burdens. On the other hand, it is true that its scope is broad and that the burdens imposed can still be considerable (and increased significantly during the legislative process[149]). The central issue in striking the balance in this respect is perhaps that the aim of facilitating innovation does not necessarily translate into a need to interpret the DSA's provisions restrictively. What is good for a given service provider is not necessarily good for innovation; innovation should be viewed from the perspective of the users and society at large. The DSA's aim of facilitating innovation should arguably especially play a role when interpreting the many open norms that it contains, in accordance with the principle of proportionality. Thus, account should be taken, *inter alia*, of the means and capacities of the service providers concerned, so that start-ups and smaller players do not necessarily carry the same burdens as larger ones. Accordingly, for instance, what is "expeditious" action upon receiving a notice, what are "diligent" steps to combat misuse, or what are "appropriate and proportionate measures" to protect minors may not always be the same for all service providers subject to the provisions in question.[150]

### B.3. Evolution

In addition to diligence and balance, the DSA's third key word is evolution. That is apparent, first of all, when we consider the origin of its provisions. The DSA may be a big deal, but it did not come about in a big bang, in the sense that its content comes out of the blue. Some provisions codify and uniformize industry practices developed over the past decades. These had often previously been enshrined in voluntary codes of conduct[151] and in EU soft law.[152] On certain points, pre-existing CJEU case law was also incorporated.[153] Most importantly, as already touched upon in Part I, the DSA borrows quite extensively from other acts of EU law.[154]

[149] By means of a rough illustration: the number of articles in the DSA increased from 74 to 93 during the legislative process, whilst the total word count (articles only) went from about 19,000 to about 35,000 words.

[150] See, respectively, Arts. 6(1), 23(3) and 28(1) DSA.

[151] See, e.g., the 2016 Memorandum of understanding on the sale of counterfeit goods on the internet, available via https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/enforcement-intellectual-property-rights/memorandum-understanding-sale-counterfeit-goods-internet_en (containing provisions on matters like notice and takedown procedures and repeat infringers).

[152] See, in particular, Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online (OJ L 63, 6.3.2018, p. 50), points 5-17 and 25-27 (containing provisions on notice and action procedures, redress, transparency, and trusted flaggers).

[153] See, in particular, C-682/18 and C-683/18, *YouTube and Cyando*, paras. 109 and 115 (on matters relating to the processing of notices and "Good Samaritan" actions).

[154] That goes for the DSA's concepts of intermediary services, the conditional liability exemptions, and the prohibition of imposing general monitoring obligations (Arts. 3(g), 4-6 and 8), all taken from the e-Commerce Directive (Arts. 12-15); the DSA's provisions on giving reasons, redress,

The reliance on the concepts and content of other acts of EU law has two implications. First, even if there is obviously no automatic parallelism considering the specific content, context, and aims of the DSA, the manner in which the relevant provisions of other acts of EU law are interpreted may have consequences for the interpretation of the DSA (and *vice versa*). Second, other institutional actors than those designated under the DSA, such as the European Data Protection Board, may have an indirect say on how the DSA is to be understood and applied. These potentially relevant actors are added to the already remarkably long lists of parties involved in the application of the DSA. That list includes – besides the services providers themselves – public bodies such as the Commission, national supervisory authorities (especially, Digital Services Coordinators[155]), the European Board for Digital Services,[156] and EU and national courts, as well as private sector operators or NGOs like trusted flagger organizations, out-of-court dispute settlement bodies, auditors, and vetted researchers.[157] In many ways, this involvement of such a broad range of parties may be one of the DSA's strengths, as it ensures a variety of perspectives, broad legitimacy, and possible synergies. Yet, it also carries risks of inconsistencies and divergent views.

There is also a second way in which the DSA embodies an approach centered on evolution. Its provisions may be relevant on their own, but the DSA is particularly noteworthy for the manner in which it weaves together several provisions into a regulatory system covering entire cycles. Take, for instance, the provisions related to the content moderation conducted by service providers. In this respect, the DSA seeks to cover the full cycle. As noted, service providers are required to provide clarity upfront in their terms and conditions about the restrictions that they apply.[158] In addition, there are requirements regarding the subsequent stages in which those restrictions are applied and enforced, including as regards the provision of reasons and the possibility of internal and external redress.[159] At the end of the cycle, service providers must provide transparency *ex post* about their content moderation practices.[160] In this manner, users can ideally take informed decisions as to their use of the service. Moreover, a virtuous feedback loop might emerge. For instance,

---

and recommender systems (Arts. 17, 20, 21, 27 and 38), inspired by the P2B Regulation (Arts. 4, 11 and 12); and the DSA's rules on service providers' contractual restrictions and the notification of suspicions of criminal offences (Arts. 14(4) and 18), based on the TCO Regulation (Arts. 5(1) and 14(5)). Furthermore, as noted, the DSA occasionally relies on concepts from other EU legislation, notably the GDPR (Arts. 25(2), 26(3), 28(2), 38, 40(8) and (13) DSA). And the DSA's provisions dealing with enforcement (Chapter IV, Section 4) echo not only those of Regulation 1/2003 (Chapters III-VII), and therefore indirectly those of the DMA (Chapter V), but on some points also those of the GDPR (Arts. 61 and 62).

[155] Art. 49 DSA.

[156] Arts. 61-63 DSA.

[157] See, respectively, Arts. 22, 21, 37 and 40(4) DSA.

[158] Art. 14(1) DSA.

[159] Arts. 14(4), 16(5), 17, 20 and 21 DSA.

[160] Arts. 14(1), 15 and 24 DSA.

service providers may conclude as a consequence of the redress decisions that certain provisions of their terms and conditions, or the manner in which they are enforced, need revision.

A similar logic underpins the DSA's rules on risk management, which are applicable only to very large service providers. They must annually assess the systemic risks associated with the provision of their services and, based on the outcome thereof, take mitigating measures.[161] Moreover, there is a system of both internal (compliance officers[162]) and external (independent auditors, vetted researchers[163]) overview and verification of these service providers' actions. Again, there is mandatory transparency reporting *ex post*.[164] In this manner, the risk assessments can build on each other, whereby account can be taken of the effects of earlier risk mitigation measures. There are also mechanisms to share best practices between the different service providers concerned.[165] Moreover, the findings of the auditors and vetted researchers can be expected to feed into this process.

Finally, at the more fundamental level, another evolution is worth noting, too. The *laissez-faire* approach of the e-Commerce Directive, referred to earlier,[166] had been pioneered in the U.S.[167] As a consequence of this approach, the question whether and, if so, to which extent due diligence was to be exercised vis-à-vis users was logically primarily answered by the service providers themselves, mostly in view of commercial considerations.[168] In many ways, having regard to the increased importance of the digital services concerned mentioned earlier, the DSA embodies an attempt to ensure that that question is instead principally answered by public bodies, in function of public policy considerations. At the same time, the service providers retain a margin of maneuver as a consequence of the DSA's focus on procedure,[169] its sometimes broadly worded norms,[170] and the space it leaves for co-regulatory

---

[161] Arts. 34 and 35 DSA.

[162] Art. 41 DSA.

[163] Arts. 37 and 40(4) DSA.

[164] Art. 42 DSA.

[165] Art. 35(2) and (3) DSA.

[166] See Part I, Section B, above.

[167] In particular, US Code Section 230 (Communications Decency Act) and Section 512 (Digital Millennium Copyright Act). See further, e.g., J.P. Quintais (ed.), 'From the DMCA to the DSA: a Transatlantic dialogue on online platform regulation and copyright,' Verfassungsbooks 2024; F. Wilman, *The responsibility of online intermediaries for illegal user content in the EU and the US*, Edward Elgar 2020, pp. 97–167.

[168] The considerations tend to involve seeking to satisfy users' expectations, but they can also relate to considerations such as not estranging advertisers, avoiding negative publicity, and responding to pressure from civil society and governments.

[169] E.g., whilst the DSA sets certain procedural rules regarding the service providers' content moderation policies (Art. 14), it remains in principle for the service providers to determine the content thereof and the means of enforcement.

[170] Such norms, firstly, allow for keeping pace with changing circumstances and, secondly, leave the service providers some scope to determine the specific measures needed to achieve the result sought, in accordance with their freedom to conduct a business. Cf., e.g., C-401/19, *Poland v. EP and Council*, para. 74.

solutions.[171] It will be interesting to see whether this evolution towards imposing a degree of public control over the provision of digital services that are essential to many aspects of modern-day life will extend further, both in terms of the degree of descriptiveness potentially being increased in the future and in the sense that the EU's approach might spill-over to third countries either through a de jure or a de facto "Brussels effect."[172]

## C. The Commission's roles under the DSA

### C.1. The Commission as implementor

Under the DSA the Commission has essentially three roles: implementor, designator, and supervisor. Its role as an implementor – which entails, in essence, doing everything that needs to be done at EU level to ensure the proper implementation of the DSA – is a classic one, in the sense that it plays this kind of role under many other pieces of EU legislation. Under the DSA the role is nonetheless rather extensive. It includes diverse activities such as acting as a repository of information,[173] chairing and supporting the European Board for Digital Services,[174] helping to solve disagreements between public authorities involved in enforcement,[175] and contributing to the co-regulatory solutions mentioned above.[176]

Yet, this role principally entails the Commission giving effect to the DSA's numerous empowerments to adopt guidelines and delegated and implementing acts.[177] Especially the delegated acts and guidelines can play an important role in giving further substance to the DSA provisions in question. The relevant empowerments can mainly be found in provisions that either were added during the legislative process and are in themselves not particularly clear,[178] or concern "the highest standard of due diligence obligations"[179] that the DSA imposes on very large service providers.[180]

---

[171] See Arts. 44-48 DSA (regarding non-binding standards and codes of conduct).

[172] A. Bradford, *The Brussels Effect: How the European Union Rules the World*, OUP 2020.

[173] E.g., Arts. 21(8), 22(4) and (5) and 24(5) DSA.

[174] Art. 61 DSA.

[175] Art. 59 DSA.

[176] Arts. 44-48 DSA.

[177] See Arts. 33(2) and (3), 40(13), 43(4) and 37(7) (empowerments for delegated acts); Arts. 15(3), 24(6), 43(3), 83 and 85(3) (empowerments for implementing acts); Arts. 22(8), 25(3), 28(4), 35(3) and 39(3) (empowerments for guidelines). Note that the Commission can, in principle, also issue guidelines without an express empowerment.

[178] In particular, Arts. 25 and 28 DSA (on "dark patterns" and the protection of minors, respectively).

[179] Rec. 76 DSA.

[180] Arts. 33, 35, 37, 39, 40 and 43 DSA (all of which are part of Chapter III, Section 5, i.e., the rules applicable specifically to very large online platforms and very large online search engines).

The Commission is currently still in the process of giving effect to all the empowerments.[181] Its priorities included ensuring its own supervisory capacities under the DSA. To that aim, it adopted not only an implementing act concerning its enforcement powers,[182] but also a delegated act on the supervisory fees to be paid by the very large service providers subject to Commission supervision.[183] The funds thus obtained help pay for the exercise of the Commission's supervisory tasks under the DSA.[184] Some service providers have challenged the subsequent implementing decisions requiring them to pay the fee, calling into question the manner in which it was calculated.[185] Those cases were still pending at the time of writing.

The Commission has also adopted an implementing act on transparency reporting and a delegated act on auditing.[186] Additional measures, especially the delegated acts on access to data and on calculating the number of average monthly active users,[187] were still to be adopted at the time of writing. In April 2024, ahead of the European Parliament elections, guidelines were issued on the mitigation of risks for electoral processes in the context of the DSA's risk management obligations.[188] To date, no further formal Commission guidelines have been adopted, although guidelines on the protection of minors are expected for the first half of 2025.[189] The revised Code of Practice on Disinformation, agreed in June 2022 and soon to become a code of conduct under the DSA, is also worth mentioning here.[190]

---

[181] Some of the empowerments prescribe consultation of the European Board for Digital Services, referred to in Art. 61 DSA, which logically first had to be established and be operational.

[182] Commission Implementing Regulation (EU) 2023/1201 of 21 June 2023 on detailed arrangements for the conduct of certain proceedings by the Commission pursuant to Regulation (EU) 2022/2065 of the European Parliament and of the Council (OJ L 159, 22.6.2023, p. 51).

[183] Commission Delegated Regulation (EU) 2023/1127 of 2 March 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council with the detailed methodologies and procedures regarding the supervisory fees charged by the Commission on providers of very large online platforms and very large online search engines (OJ L 149, 9.6.2023, p. 16). On supervisory fees, see Art. 43 DSA.

[184] See Rec. 101 DSA.

[185] See Cases T-55/24, *Meta v. Commission*; T-58/24, *TikTok v. Commission* (both pending).

[186] See, respectively, Commission Implementing Regulation (EU) 2024/2835 of 4 November 2024 laying down templates concerning the transparency reporting obligations of providers of intermediary services and of providers of online platforms under Regulation (EU) 2022/2065 of the European Parliament and of the Council (OJ L, 2024/2835, 5.11.2024); Commission Delegated Regulation (EU) 2024/436 of 20 October 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines (OJ L, 2024/436, 2.2.2024).

[187] At the end of 2024, the Commission launched a public consultation on the former delegated act. See https://digital-strategy.ec.europa.eu/en/news/commission-launches-public-consultation-rules-researchers-access-online-platform-data-under-digital

[188] Commission, Guidelines for providers of very large online platforms and very large online search engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065, C/2024/3014, 26.4.2024.

[189] See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines_en

[190] Commission, Press release IP/25/505, 13 February 2025. See https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

### C.2. The Commission as designator

As noted, the DSA imposes the most demanding due diligence obligations only on providers of very large services – specifically, on very large online platforms and very large online search engines. Those obligations – unlike the DSA's other obligations – become applicable only upon designation of the service in question. Unlike under the DMA, under the DSA designation depends on a single criterion, without there being any rebuttable presumptions,[191] namely, exceeding the threshold of 45 million average monthly active users in the EU.[192] Although the DSA's definitions[193] and recitals[194] and the Q&A document that the Commission published in 2023 all help increase clarity,[195] determining the number of average monthly active users is not necessarily as straightforward as it may sound. Challenges arising in this connection include precisely how such numbers should be calculated and whose data should be used for these purposes, as well as how to deal with "hybrid" services that are used not only by third parties, but also by the service provider itself, to sell certain goods or services to users.[196]

To date, the Commission has designated 25 services as either very large online platforms or as very large online search engines.[197] Those services include, among others, Zalando, Wikipedia, Google Search, Bing, Amazon, LinkedIn, YouTube, Facebook, Instagram, TikTok, and X.

Several service providers challenged the Commission implementing decisions by which their respective services were designated.[198] In all cases, the main actions are currently still pending. However, some service providers also brought proceedings for interim measures. The leading case is the one brought by Amazon seeking the suspension of the designation decision relating to its marketplace service in so far as it concerns the DSA's obligations regarding recommender systems and advertising transparency.[199] Amazon was initially partly successful: the President of the General Court ordered the suspension of the advertising transparency obligation, which entails service providers compiling and making publicly available a repository containing information on the

---

[191] Unlike under the DMA. See Part III, Section B.3, below.

[192] Art. 33(1) DSA.

[193] See in particular Art. 3(m), (p) and (q) DSA.

[194] Rec. 77 DSA.

[195] See https://digital-strategy.ec.europa.eu/en/library/dsa-guidance-requirement-publish-user-numbers

[196] See further, e.g., M. Husovec, *Principles of the Digital Services Act*, OUP 2024, pp. 168–171; F. Wilman, 'Article 33: Very large online platforms and very large online search engines,' in: Wilman, Kalėda and Loewenthal, n. 110 above, pp. 250–252.

[197] See https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses

[198] In addition to the cases mentioned below, see Cases T-348/23, *Zalando v. Commission*; T-134/24, *Technius v. Commission*; T-138/24, *Aylo Freesites v. Commission*; T-139/24, *WebGroup v. Commission*; T-486/24, *NKL Associates v. Commission* (all pending).

[199] Arts. 38 and 39 DSA.

advertisement presented on their services.[200] The order was essentially based on the view that the information, presumed to be sensitive, that is disclosed in this manner could subsequently not be "undisclosed" should Amazon succeed in the main action. However, on appeal the Vice-President of the Court of Justice ruled differently and lifted the suspension. In particular, the latter gave more weight to the public interest associated with ensuring advertising transparency and also took account of the unequal playing field that would result from suspending the obligation only in respect of Amazon.[201]The designation-based approach on which the DSA partially relies is also followed by the DMA, yet it is quite rare in EU law generally. It has considerable advantages. Most notably, it enables targeted interventions (covering precisely the services that are deemed in need of regulation), allows for a degree of dynamism (services designated can also be "un-designated"), and provides clarity and legal certainty (it is clear to all which services are covered). The initial experiences gathered seem to indicate that this approach works rather well. Nonetheless, it involves transaction costs of various types. To make it possible to determine which services might need to be designated, all relevant service providers must publish their number of average monthly active users.[202] There are naturally also costs involved in the designation process itself. Moreover, the approach inherently creates challengeable acts, namely the designation decisions.[203] As has been seen, the service providers concerned are not shy to challenge those decisions in court. Unsurprisingly, given what is at stake, they sometimes use this opportunity not to call into question the designation as such, but rather – as, for instance, in the Amazon case mentioned – the application to them of certain specific due diligence obligations.[204]

### C.3. The Commission as supervisor: first impressions

The DSA attributes important supervisory tasks to the Commission.[205] The latter is exclusively competent for supervising providers of very large services'

[200] Order President General Court Case T-367/23 R, *Amazon v. Commission*, EU:T:2023:589.

[201] C-639/23 P(R), *Commission v. Amazon*. See also Cases C-511/24 P(R) (appeal T-138/24 R) and C-620/24 P(R) (appeal T-139/24 R).

[202] Art. 24(2) DSA.

[203] The Commission had proposed attributing the task of taking designation decisions to the competent national authorities, meaning that litigation would have taken place at national level, but the EU legislator decided to attribute it to the Commission instead. See Commission, Proposal for a Regulation of the European Parliament and of the Council on a single market for digital services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, COM(2020) 825, p. 59 (Art. 25).

[204] Indeed, it may be no coincidence that Amazon's action for interim measures, and those of several other service providers, focused specially on the DSA obligations regarding recommender systems and advertising, considering the importance of those two topics for many of the services covered.

[205] Art. 56 DSA.

compliance with the DSA obligations that apply only to them.[206] In respect of their compliance with all other DSA obligations, the Commission shares competence with the relevant authorities designated by the Member States, in particular their Digital Services Coordinators. However, those national authorities are competent only where the Commission has not initiated proceedings for the same infringement.[207] All other – that is, not "very large" – services covered by the DSA are solely subject to supervision by the national authorities of the Member State of their main place of establishment (or, where relevant, that of their legal representative[208]).

It is currently too early to draw conclusions on the exercise of the Commission's supervisory tasks. Nonetheless, as a first impression, it seems fair to say that the Commission has energetically taken up these tasks. Having sent numerous requests for information to the providers of many of the (at present) 25 very large services under its supervision on a broad range of topics, to date it has opened in total nine formal proceedings to investigate possible violations in respect of six of those services.[209] One of them, concerning X, has resulted in preliminary findings.[210] Moreover, one of the investigations has already been concluded. That investigation concerned a new functionality – the TikTok Lite programme – that Bytedance intended to launch in certain Member States. The Commission took the view that a prior risk assessment and mitigation exercise should have been conducted, in particular in the light of concerns about the potentially addictive effects of the new functionality, including for minors.[211] In the light of the Commission's concerns, Bytedance committed to permanently withdrawing that functionality from the EU. The Commission made the commitments binding, thus bringing the proceedings to an end.[212]

In fact, many of the aforementioned investigations involve alleged violations of the DSA's risk assessment and mitigation obligations.[213] This illustrates both the centrality and the broad scope of those obligations. It also illustrates that whilst, as was discussed above, gradual evolution is an important feature of the risk management system, in the Commission's view this does not rule out

[206] That is, the obligations laid down in Chapter III, Section 5, DSA.

[207] Cf. Rec. 125 DSA (stating that the Commission should normally deal with systematic infringements and Member States with individual infringements).

[208] See Art. 13 DSA (regarding service providers without an establishment in the EU).

[209] The six services subject to investigations are X, TikTok, AliExpress, Facebook, Instagram, and Temu, some of them being subject to several investigations. In addition to the press releases cited in the other footnotes, see Commission, Press release IP/23/6709, 18 December 2023; Press release IP/24/926, 19 February 2024; Press release IP/24/1485, 14 March 2024; Press release IP/24/2664, 16 May 2024; Press release IP/24/3761, 12 July 2024; Press release IP/24/5622, 31 October 2024.

[210] Commission, Press release IP/24/3761, 12 July 2024.

[211] Commission, Press release IP/24/2227, 22 April 2024. Pursuant to Art. 34(1) DSA, risk assessments are to be conducted not only annually, but also "prior to deploying functionalities that are likely to have a critical impact on the risks identified."

[212] Commission, Press release IP/24/4161, 5 August 2024.

[213] Arts. 34 and 35 DSA, at stake in seven of the nine investigations (sometimes combined with other alleged violations).

holding service providers accountable for failures in individual cases. Possible violation of the DSA's data access obligations is another recurring topic in the investigations.[214] This arguably illustrates service providers' hesitance to give insights into what happens "under the hood" when it comes to some of their core activities, such as the workings of their recommender systems and their data-related practices. Although somewhat less frequently at stake, other possible breaches under investigation relate to notice and action mechanisms, the protection of minors, and advertising transparency.[215] It thus appears that many of the obligations at stake involve the "protective diligence" requirements of the type mentioned earlier.

Perhaps the most eye-catching ongoing investigation concerns the one into TikTok's suspected failure to properly assess and mitigate systemic risks linked to election integrity in the context of the Romanian presidential elections on 24 November 2024.[216] Manipulation and foreign interference, especially on TikTok, was an important reason for the annulment by Romania's constitutional court of the result of the first round of voting and its order to restart the process rather than to proceed with the second round.[217] In this connection the Commission issued a retention order, requiring the preservation of data related to systemic risks this service could pose on electoral processes and civic discourse in the EU (and therefore not only in Romania).[218] The European Parliament, too, got involved in the discussions.[219] This investigation came on top of earlier investigatory proceedings in respect of Facebook and Instagram, both provided by Meta, for activities relating to civic discourse and electoral processes, specifically in connection to the European Parliament elections of June 2024.[220] Whilst also involving other concerns, the latter investigation turns in particular on Meta's decision to phase out a tool called CrowdTangle, which enabled real-time election monitoring for researchers, journalists, and civil society organizations.

### C.4. The Commission as supervisor: underlying issues

Views on the DSA's system of public enforcement are likely to differ considerably depending on one's point of view. Persons familiar with EU competition law might find it hardly noteworthy, since in this respect the DSA resembles – and has indeed been inspired by – Regulation 1/2003. However, those viewing

[214] Art. 40 DSA, at stake in six investigations.
[215] Arts. 16, 25 and 39 DSA, respectively, at stake in three of four investigations.
[216] Commission, Press release IP/24/6487, 17 December 2024.
[217] See n. 107 above.
[218] Commission, Press release IP/24/6243, 5 December 2024.
[219] "We are getting fed up': EU lawmakers snap at TikTok over Romanian election,' *Politico*, 3 December 2024.
[220] Commission, Press release IP/24/2373, 30 April 2024.

the system from the angle of EU internal market law may well find it remarkable, given that in the latter domain the DSA's approach is a novelty. Considering that under the DMA (strictly speaking also an internal market measure) the Commission is the principal supervisor and that also the more recently adopted Artificial Intelligence (AI) Act attributes certain supervisory tasks to the Commission,[221] we might be witnessing the emergence of a new model for the enforcement of "Big Tech"-related internal market legislation in which the Commission plays a central role.

It is noteworthy that, in its proposal for the DSA, the Commission had proposed a more limited supervisory role for itself.[222] In contrast to what occurred in connection to the DMA,[223] especially the Member States gathered in the Council argued for increasing the Commission's role in this respect under the DSA.[224] The main reason appears to have been dissatisfaction with the functioning of the country-of-origin principle, which is enshrined in e-Commerce Directive[225] and essentially also in the GDPR,[226] where it has not always functioned fully satisfactorily.[227] Moreover, there is a certain logic to subjecting the largest digital service providers, which tend to operate in a pan-European way, to oversight by a centralized, pan-European body such as the Commission.

That does not mean, however, that the choice to attribute important supervisory tasks to the Commission is without challenges. Some of these are mainly practical. There were, for instance, concerns about the Commission having the necessary expertise and resources. The DSA seeks to address these by measures like the imposition of the aforementioned supervisory fees as well as an emphasis on cooperation and mutual assistance.[228] Within the Commission, DSA supervision and enforcement is principally done by the Platforms Directorate set up within its Directorate-General for Communications Networks, Content and Technology (DG CNECT), assisted by the Legal Service. The Commission reported that, by the end of 2023, it had spent around 27 million euros on this task and the responsible team consisted of 69 persons.[229]

[221] Art. 75 AI Act.

[222] See Commission, Proposal for a Regulation of the European Parliament and of the Council on a single market for digital services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, COM(2020) 825, pp. 68–69 (Art. 40) and pp. 75–77 (Arts. 50-51).

[223] See Part III, Section E, below.

[224] See Council, General approach on the DSA, 18 November 2021, 13203/21 (Art. 44a).

[225] Art. 3 e-Commerce Directive.

[226] Art. 56 GDPR.

[227] See, e.g., Commission, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition: two years of application of the General Data Protection Regulation,' COM(2020) 264, 24 June 2020, p. 5 (stating that further progress is needed to make the handling of cross-border cases more efficient and harmonized across the EU). See further Husovec, n. 196 above, pp. 420–421.

[228] See, in particular, Arts. 56(5) and 57 DSA.

[229] See Commission, Report on the overall annual costs incurred for the fulfilment of the Commission's tasks pursuant to Regulation (EU) 2022/2065 in the period from 16 November 2022 until 31 December 2023 and the total amount of the annual supervisory fees charged pursuant to Article 6(4) of Commission Delegated Regulation (EU) 2023/1127 in 2023, COM(2024) 523, 6 November 2024.

A Centre for Algorithmic Transparency and a DSA whistleblower tool have also been established.[230] Any practical challenges experienced in the process of taking on its supervisory tasks appear not to have substantially hindered the Commission in the exercise of those tasks.

Given that national supervisory authorities still play an important role and that digital services can easily be provided across borders, effective cooperation between the different supervisory authorities is likely to be essential to make a success of DSA enforcement. The DSA contains several measures to this effect, such as the provisions on cross-border cooperation and joint investigations.[231] In addition, the European Board for Digital Services offers a forum for cooperation and information exchange. Time will tell whether these measures are sufficient or whether additional ones might be called for, as occurred in the field of competition law and in connection to GDPR enforcement.[232] The Commission, for its part, is already working together with national supervisory authorities – notably with the Irish one, Ireland being the Member State where many of the service providers concerned are established – when conducting some of the abovementioned investigations.[233]

More principled issues have arisen too. These relate particularly to the risk of DSA enforcement being seen as "politicized."[234] There is no doubt that the DSA – and therefore also DSA *enforcement* – can raise issues that are highly political in nature. The annulment of the Romanian elections because of manipulation and foreign interference via TikTok, mentioned earlier, is but one powerful illustration thereof. Moreover, as noted, the DSA relies on open norms in several key provisions, including those on risk assessment and mitigation, thus leaving a degree of discretion. That being so, there is a risk of perceptions arising that "political" considerations might have played a role in the decision-making.

---

[230] See, respectively, https://algorithmic-transparency.ec.europa.eu/index_en and https://digital-strategy.ec.europa.eu/en/policies/dsa-whistleblower-tool

[231] Arts. 58 and 60 DSA.

[232] See Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market (OJ L 11, 14.1.2019, p. 3); Commission, Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM(2023) 348, 4 July 2023.

[233] According to the relevant press releases, that goes for the aforementioned investigations relating to TikTok and Temu, initiated on 31 October 2024 and 17 December 2024, respectively.

[234] See, e.g., I. Buri, 'A regulator caught between conflicting policy objectives: reflections on the European Commission's role as DSA enforcer, in: Van Hoboken et all (eds.), n. 104 above, pp. 75–89, at p. 85 (noting that content moderation is highly contested and politicised and arguing that questions connected to the perceived legitimacy of the Commission in overseeing the regulation of these matters might have been underestimated); Access Now, ARTICLE 19 and Electronic Frontier Foundation, 'Civil society statement: Commissioner Breton needs to stop politicising the Digital Services Act,' 19 August 2024, available via https://www.accessnow.org/press-release/commissioner-breton-stop-politicising-digital-services-act

The Commission's independence is anchored in the Treaties.[235] Yet perceptions can matter, too. It may well be in the Commission's own interest to dispel any perception of politization as much as possible. It could do so, for instance, by being predictable and transparent – concretely, by being clear upfront about its enforcement priorities and by publishing annual activity reports *ex post*.[236] Fleshing out what, in its view, service providers are expected to do exactly under broadly worded provisions such as those on risk assessment and mitigation should help too. Other conceivable measures could include setting up a panel of independent experts to advise on sensitive cases and to appoint a hearing officer to help ensure impartiality and objectivity in the DSA enforcement proceedings.[237] It is not excluded that, in the longer run and depending on the experiences gathered, the question of whether a separate body ought to be charged with EU-level DSA enforcement might re-emerge – that option having been rejected whilst the DSA was being prepared, mainly due to the costs and time constraints.[238]

Additional challenges might result from the changing political winds blowing across the Atlantic, which might entail push-back against attempts to enforce the DSA in respect of U.S.-based service providers.[239] In that regard, some may see it as disadvantageous that the DSA attributes to the Commission enforcement tasks in respect of very large service providers, many of which are headquartered in the U.S. For this might involve a risk of the performance of those tasks being intertwined – or being *seen* as intertwined – with some of the Commission's other responsibilities, such as those under the EU's trade or security policies. However, apart from the fact that the Commission has not only a clear responsibility but also a clear interest in adequately performing its tasks under the DSA, it is probably better placed to withstand any such external pressure than the competent authority of an individual Member State would be. The DSA reflects the idea that, by acting collectively, Europeans are better able to stand up to "Big Tech." That logic holds irrespective of whether the latter exercise pressure directly, for instance through threats to end their service provision,[240] or indirectly, through the government of their home country.

---

[235] See, in particular, Art. 17 TEU. Cf., e.g., W. Wils, 'The independence of competition authorities: the example of the EU and its Member States,' *World Competition* 42 2019, p. 149 (expanding on the Commission's independence in a competition law context).

[236] Cf. Art. 55 DSA (obliging national supervisory authorities to draw up annual activity reports).

[237] Cf. Decision 2011/695/EU of the President of the European Commission of 13 October 2011 on the function and terms of reference of the hearing officer in certain competition proceedings (OJ J L 275, 20.10.2011, p. 29).

[238] Commission, Impact assessment DSA (part 1/2), SWD(2020) 348, 15 December 2020, pp. 71 and 73. See also Husovec, n. 196 above, p. 425.

[239] E.g., 'JD Vance says US could drop support for NATO if Europe tries to regulate Elon Musk's platforms,' *Independent*, 17 September 2024; 'Zuckerberg urges Trump to stop the EU from fining US tech companies,' *Politico*, 11 January 2025

[240] E.g., 'Google threatens to withdraw search engine from Australia,' *BBC News*, 22 January 2021; 'Facebook and Instagram to restrict news access in Canada,' *BBC News*, 23 June 2023.

## D. Specific issues

### D.1. Private enforcement

Article 54 DSA deals with the possibility of users to seek – and, where the relevant conditions are met, naturally also *obtain* – compensation for any damage or loss suffered due to service providers' infringements of their obligations under the DSA.

This article is helpful, first, in that it clarifies what already results from primary EU law, namely, that such a right to compensation exists.[241] Second, it articulates the three conditions that apply for this right to arise, that is, the existence of an infringement, damage, and a causal link between the two.[242] Third, it makes clear that "any damage or loss" is compensable, covering therefore both material and immaterial damage.[243] Whilst less clearly articulated, it can safely be assumed that users have a right to full compensation of the damage or loss actually suffered – no less, but no more, either.[244]

Article 54 DSA underlines the need to exercise the users' right to compensation in accordance with EU and national law. That means, on the one hand, that the fundamental right to effective judicial protection, enshrined in Article 47 Charter, and the EU law principles of effectiveness and equivalence must be respected. On the other hand, provided EU law is complied with, pursuant to the principle of national procedural autonomy, national law plays an important role in operationalizing this right, for instance concerning the quantification of the loss or damage suffered.[245] As seen in other domains, such quantification can be challenging in practice.[246] Especially considering that under the DSA users will often be consumers and that the harm can be limited at individual level, it is relevant to note that the Representative Actions Directive also covers infringements of the DSA.[247] In addition, the DSA contains its own rules on the possible representation of users by specific bodies.[248]

---

[241] Cf., e.g., Case C-295/04, *Manfredi*, EU:C:2006:461 (regarding competition law).

[242] Cf., e.g., Case C-300/21, *Österreichische Post*, EU:C:2023:370, para. 32 (regarding the GDPR); Case C-295/04, *Manfredi*, para. 61 (regarding competition law).

[243] Cf., e.g., Case C-99/15, *Liffers*, EU:C:2016:173, para. 26 (regarding intellectual property law).

[244] Cf., e.g., C-300/21, *Österreichische Post*, para. 58; C-99/15, *Liffers*, para. 25. See, however, also C-295/04, *Manfredi*, para. 99 (indicating that the principle of equivalence could necessitate the possibility to award punitive damages).

[245] E.g., C-300/21, *Österreichische Post*, para. 54; C-295/04, *Manfredi*, para. 98.

[246] Cf., e.g., Commission, Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights, COM(2017) 708, 29 November 2017, p. 3 ("Practice shows that assessing damages for infringement of [intellectual property rights] can be complicated"). See also Commission, Communication on quantifying harm in actions for damages based on breaches of Article 101 or 102 TFEU (OJ C 167, 13.6.2013, p. 19).

[247] 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 (OJ L 409, 4.12.2020, p. 1). See Art. 90 DSA.

[248] Art. 86 DSA.

The DSA expressly provides for the possibility of the Commission making written or oral submissions before national courts, but only in connection to proceedings to temporarily restrict the access to the online interfaces of service providers engaged in certain persistent and serious infringements.[249] In this respect the DSA is thus more restrictive than Regulation 1/2003, which provides for that possibility in a more general manner.[250] Perhaps this difference can be explained by the fact that, as mentioned, the Commission was only attributed full-blown enforcement powers during the legislative process. In any event, it probably means that the Commission's involvement in national proceedings is dependent on the competent national courts having requested its assistance, in accordance with the CJEU's case law.[251]

The Commission's role in DSA enforcement means that there is scope for "follow-on" actions of the type known in competition law, that is, damages claims brought at national level after the Commission established an infringement at EU level. This can have implications for matters such as the application of limitation periods provided for in national law.[252] Echoing Regulation 1/2003, the DSA expressly provides for the binding effect of Commission decisions.[253] There is no equivalent of the rule of the Competition Damages Directive on the effects of decisions taken by national supervisory authorities.[254]

Finally, the DSA seems to illustrate a broader issue with private enforcement of EU law, namely, that it is often somewhat of an afterthought. Article 54 DSA was only added during the legislative process. There is also little consistency in the EU legislature's approach.[255] For instance, it is hard to explain why the DMA contains no similar provision, whilst the corresponding provision in the GDPR is drafted differently.[256] Moreover, Article 54 DSA does not cover all private enforcement-related issues that can emerge. There might even be a risk of it – wrongly – being read *a contrario*. For example, the article should not be understood as implying that damages claims are necessarily the *only* type of private enforcement actions possible. In all likelihood, other types of actions, such as those for injunctions, are in principle possible too.[257] Furthermore,

[249] Art. 82(2), read in conjunction with Art. 51(3), DSA.

[250] Art. 15 Regulation 1/2003.

[251] Order Case C-2/88 Imm., *Zwartveld*, EU:C:1990:315.

[252] E.g., Case C-605/21, *Heureka Group*, EU:C:2024:324.

[253] Art. 82(3) DSA. See Art. 16(1) Regulation 1/2003.

[254] Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union (OJ L 349, 5.12.2014, p. 1), Art. 9.

[255] See, more generally, F. Wilman, *Private enforcement of EU law before national courts: the EU legislative framework*, Edward Elgar 2015, pp. 437–442 and 560–564.

[256] Art. 82(1) GDPR.

[257] Cf., e.g., Case C-253/00, *Muñoz*, EU:2002:497. See also Husovec, n. 196 above, p. 428; S. Kalėda, 'Article 54: Compensation,' in Wilman, Kalėda and Loewenthal, n. 110 above, p. 371; A. Komninos, 'Private enforcement of the DMA rules before national courts,' 2024, available via https://ssrn.com/abstract=4791499 (all taking a similar view, the latter in connection to the DMA). See also Part III, Section F, below.

it seems not excluded that other parties than users can also bring claims against service providers for violation of the relevant DSA obligations. Think, for instance, of trusted flaggers organizations or (vetted) researchers.[258]

### D.2. Out-of-court dispute settlement

In addition to the public and private enforcement discussed above, the DSA also provides for what could be called "privatized" enforcement. Its Article 21 constitutes the basis for the establishment of out-of-court dispute settlement (ODS) bodies. Users can turn to one of these bodies when they disagree with content moderation decisions taken by the service providers covered, such as the removal of information, suspension of the users' accounts, or restrictions of their ability to monetize information. Users will at most be charged a nominal fee, which they can recover if the body decides in their favour. In practice, service providers are likely to bear most, if not all, of the costs.[259]

Under the DSA, ODS bodies need prior certification by the competent national authorities. This is meant to ensure that they are independent and have the necessary expertise and that the proceedings are fair and efficient. At the time of writing, six bodies had been certified, in France, Ireland, Germany, Hungary, Malta, and Italy.[260] The certified bodies have different areas of expertise, and most are capable of settling disputes in several languages. Still, so far, they offer proceedings in only nine of the EU's 24 official languages. This underlines the point that civil society uptake is crucial to fully realize the DSA's potential across the EU.[261] Article 21 DSA provides for the option – but not the obligation – for Member States to step in and either set up ODS bodies themselves or to support the activities of existing bodies.

In essence, Article 21 DSA seeks to offer users a quick, simple, and cheap means of redress. That is particularly important in the present context, given the characteristics of the typical disputes covered. Often the users concerned are consumers (thus having limited resources and expertise) and the disputes may well involve only relatively modest harm (expressed in monetary terms) and be time-sensitive (in that they become moot if it takes too long to resolve them). As importantly, especially for very large service providers, the disputes tend to arise on a massive scale. They can take millions of content moderation decisions leading to hundreds of thousands of appeals per year.[262] Whilst the internal redress mechanisms

[258] Cf., e.g., 'German civil activists win victory in election case against Musk's X,' *Reuters*, 7 February 2025.

[259] See, e.g., D. Holznagel, 'Art. 21 DSA Has Come to Life,' *Verfassungsblog*, 5 November 2024.

[260] See https://digital-strategy.ec.europa.eu/en/policies/dsa-out-court-dispute-settlement

[261] M. Husovec, 'Will the DSA work?,' Van Hoboken et all (eds.), n. 104 above, pp. 20–33, at pp. 21–22.

[262] See, e.g., YouTube's transparency report for the period 1 March – 30 June 2024, available via https://transparencyreport.google.com/report-downloads?lu=report-27 (citing around 230.000

prescribed by the DSA may help deal with the bulk of them,[263] affected users may still feel the need for independent review. For the reasons given, "classic" judicial redress is often hardly a realistic option. ODS is meant to plug the resulting hole. Since judicial redress remains possible for affected parties, their right to an effective remedy under Article 47 Charter is not called into question.

Crucially, the ODS bodies' decisions taken under Article 21 DSA are not binding. However, the parties must engage in good faith and service providers may be under pressure to respect the outcomes.[264] Time will tell whether service providers will accept and implement the decisions to a degree sufficient to make this form of redress attractive for users. Conversely, especially if users pay no fees at all, there might be a risk of abuse. The DSA's provision on combatting misuse does not cover misuse of the ODS mechanism.[265] Instead, Article 21 DSA foresees the possibility of the ODS bodies requiring users to pay the service providers' costs where they "manifestly acted in bad faith." Whether that possibility will serve as a sufficiently effective deterrent in practice remains to be seen. It will also be interesting to see what weight, if any, national courts will give to decisions by ODS bodies when seized after a user has received an unfavourable decision or a service provider refuses to implement a favourable onFrom an institutional perspective, perhaps the most important question is that of consistency. Especially since Article 21 DSA leaves certified ODS bodies some latitude (for instance, no standard of review is specified), it is not inconceivable that different bodies develop somewhat different practices and that their decisions are not always perfectly aligned. If that were to occur on a significant scale, it would not only put affected service providers in a difficult position; it could also undermine the credibility and therefore the effectiveness of the ODS mechanism and create uncertainty about the interpretation of the relevant provisions of the DSA. It seems evident that the preliminary reference procedure is not available for ODS bodies, if only because of their lack of compulsory jurisdiction.[266] The DSA does not provide any formal mechanism to help ensure consistency in this respect.[267] Under Article 21 DSA, only in extreme cases, involving non-compliance with the applicable conditions, can national supervisory authorities step in by revoking the certification.

---

notice-based and around 30 million own initiative content moderation decisions, as well as around 400.000 complaints received).

[263] Art. 20 DSA. Note that the disputes brought under Art. 21 DSA may be preceded by such internal review, but that this is not a mandatory requirement.

[264] Cf., e.g., Art. 35(1)(g) DSA (mentioning implementing said decisions as a possible risk mitigation measure for very large service providers).

[265] Art. 23 DSA.

[266] E.g., Case C-54/96, *Dorsch Consult*, EU:C:1997:413, paras. 27-29.

[267] Interestingly, as a private initiative initiated by one of the certified ODR bodies (namely, User Rights), an "Article 21 Academic Advisory Board" has been set up, which might help reduce the risk of inconsistencies. See https://www.user-rights.org/de/advisory-board#:~:text=The%20Article%2021%20Academic%20Advisory%20Board%20discusses%20the%20most%20challenging,academics%20and%20civil%20society%20organisations

### D.3. Preemption

The last topic to be addressed in this Part II is not about enforcement but rather involves the preemptive effect of the DSA in respect of national legislation. In this connection its Recital 9 states that the DSA constitutes full harmonization and that, accordingly, Member States should not adopt or maintain additional national requirements relating to matters falling within the scope of the DSA.[268] This recital recalls in essence what already follows from settled CJEU case law, namely, that Member States are precluded in principle from adopting or maintaining national provisions in parallel to Regulations.[269] Naturally, that rule only extends to the matters covered by the Regulation in question. And it does not exclude Member States taking certain implementing measures. They may even expressly be required to do so, as occurs under the DSA when it comes to the designation and powers of national supervisory authorities and the penalties that those authorities may impose.[270]

Whilst the rule recalled in Recital 9 DSA itself is clear, its application can raise complex questions. Detailed, case-by-case assessments of both the Regulation and the relevant national rules at issue can be required to assess whether the former preempts the latter.[271] The DSA may prove particularly challenging in this regard given that its objective and scope are wide and that some of its provisions are worded in general terms. Perhaps as importantly, the field of digital service provision tends to be dynamic and give rise to politically sensitive issues. Although the broad wording of some of the DSA's provisions serves in part precisely to take account of such dynamism,[272] it is therefore nonetheless not hard to conceive of issues arising that are seen as in need of regulation and in respect of which it is not beyond debate whether they are covered by the DSA or not.

One could think, for instance, of current debates about whether minors should be prevented from having access to social media services. Such "social media bans" tend to be framed in terms of requirements addressed to the relevant service providers.[273] They raise complex legal and practical questions already in themselves, for instance regarding the effectiveness of age-verification technology and the compatibility of such bans with the rights of the child. But on top of that, debates could arise about the relationship with existing EU law, including (although not only) the DSA.[274] Similar questions can arise in

[268] See further S. Kalėda, 'Article 1: Subject matter,' in: Wilman, Kalėda and Loewenthal, n. 110 above, pp. 17–19.

[269] E.g., Joined Cases C-539/10 P and C-550/10 P, *Stichting Al-Aqsa v. Council*, EU:C:2012:711, paras. 85-87.

[270] Arts. 49-52 DSA.

[271] E.g., Case C-438/23, *Protéines France*, EU:C:2024:826, paras. 50-96.

[272] See n. 170 above.

[273] E.g., 'Australia approves social media ban on under-16s,' *BBC News*, 29 November 2024.

[274] Apart from the DSA, questions about consistency with, e.g., the GDPR (especially when it comes to age-verification tools) and the e-Commerce Directive (especially the home state control principle of its Art. 3) could arise too.

respect of national laws meant to bar minors' access to services hosting pornographic content.[275] The DSA not only evidently covers these kinds of services and seems to pursue similar aims; it also contains rules that specifically require relevant service providers to "put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors,"[276] whilst the rights of the child and the protection of minors are also part of the risk assessment and mitigation exercise.[277] At the same time, the DSA includes nothing resembling express bans of this type.

Therefore, differences of opinion could arise in connection to the DSA's preemptive effect on possible national legislation regarding these sorts of matters. Such questions are, of course, analytically distinct from the ones on the relationship between the DSA and other acts of EU law, discussed earlier.[278] However, in practice they may overlap. That could occur, for instance, where a Member States claims the national law at issue constitutes a measure to protect minors from harmful content on video-sharing platforms in implementation of the AVMSD.

Subject to political decision-making and the availability of a sufficient legal basis (normally, Article 114 TFEU on the internal market), it might in certain cases be deemed preferable to regulate the matter at EU, rather than at national, level. If so, this would likely happen in the form of a complementary, self-standing legal act. For there is probably little appetite to amend the DSA, since it has been adopted only quite recently and proposing an amendment could lead to discussions on all kinds of other topics being re-opened. Even more recently adopted legal acts such as the European Media Freedom Act and the Political Advertising Regulation are examples of such complementary legal acts. As noted in Part I, they contain certain "top-ups" to DSA provisions.[279] Yet this approach is not without downsides. At best it adds complexity and at worst it turns the DSA into something of a Christmas tree.

Alternatively, the potential differences of opinion referred to above might eventually have to be settled through infringement proceedings under Article 258 TFEU. To date, the Commission's activities in this regard have focused solely on the Member States's positive obligations under the DSA, specifically those to designate and empower national supervisory authorities.[280] However, for the reasons given, those activities might, where necessary, in time also extend to Member States' negative obligations pursuant to the principle of preemption. In that sense, this topic too might be about enforcement after all.

---

[275] See, e.g., Case C-188/24, *WebGroup* (pending, focusing on the e-Commerce Directive).

[276] Art. 28(1) DSA.

[277] Art. 34(1)(b) and (d) DSA.

[278] See Part I, Section G, above.

[279] E.g., Art. 18(4) and (5) European Media Freedom Act; Arts. 13(2) and (3) and 22(3) Political Advertising Regulation. See further Part I, Section G, above.

[280] In December 2024 the Commission sent reasoned opinions to four Member States (Belgium, Spain, the Netherlands, and Poland). See https://ec.europa.eu/commission/presscorner/detail/en/inf_24_6006

# PART III: DIGITAL MARKETS ACT (DMA)

## A. Introduction

If one had to condense the DMA into just two words, those would undoubtedly be "fairness" and "contestability." This is not just because those words appear in the title of the DMA or in its Article 1 as the two objectives that the DMA is meant to achieve. They also permeate a large part of the 109 recitals and 54 articles of which the DMA is composed and explain many of the concrete policy choices made by the EU legislature in the design of the DMA.

"Contestability" is defined in the DMA as "the ability of undertakings to effectively overcome barriers to entry and expansion and challenge the gatekeeper on the merits of their products and services."[281] Fairness can be derived, a contrario, from the DMA's definition of "unfairness," which relates to "an imbalance between the rights and obligations of business users where the gatekeeper obtains a disproportionate advantage."[282]

Weak contestability and unfairness correspond to two of the three "problem clusters" that the Commission's Impact Assessment Report found digital markets to be particularly vulnerable to, the third one being the "fragmented regulation and oversight" arising from the risk of different national legislations within the EU.[283] The risk of fragmentation is of course what justified the adoption of the DMA as a set of harmonised rules established at EU level on the basis of Article 114 TFEU.[284]

The need to remedy weak contestability and unfairness in the EU digital sector was reflected in the DMA at several levels. First, it guided the identification of the categories of core platform services ("CPSs") falling within the material scope of application of the DMA. Indeed, the ten categories of CPSs listed in Article 2, point (2), DMA refer to those digital services that are most broadly used by business users and end users and where concerns about weak contestability and unfair practices by gatekeepers were considered to be more apparent and pressing.[285] Second, the objectives of contestability and fairness also informed the three qualitative criteria that define the notion of "gatekeeper" under Article 3(1) DMA (and, as a result, the quantitative thresholds that are based on those criteria). It is only when a CPS constitutes an important gateway and is operated by an undertaking with a significant impact in the internal

[281] Rec. 32 DMA.

[282] Rec. 33 DMA.

[283] Impact Assessment Report accompanying the Commission's proposal for the DMA, SWD(2020) 363 final, Part 1/2, paras. 26-29.

[284] As explained below (Section E), the need to avoid fragmentation also explains the central role that the Commission has been given in the implementation of the DMA.

[285] This is due to features such as extreme scale economies, very strong network effects, an ability to connect many business users with many end users, lock-in effects, a lack of multi-homing or vertical integration, which characterise some of those digital services. Rec. 13-14 DMA. See also Part I, Section E.1, above.

market and an entrenched and durable position, that concerns of weak contestability and unfairness are deemed likely to arise, thereby justifying the imposition of obligations.[286] Third, and most importantly, contestability and fairness substantially inspired the design of the obligations imposed on gatekeepers under Articles 5, 6 and 7 DMA. Many of those obligations are based on concrete experience from competition law enforcement showing that certain unilateral practices by large undertakings are likely to undermine contestability and fairness in digital markets.[287]

Against this background, this Part III seeks to provide an overview of the architecture of the DMA, taking into account the experience gathered in its first 21 months of application. First, the mechanism of gatekeeper designation is examined – a crucial, and all the more contentious, requirement for the application of the DMA's obligations. Second, focus is placed on those obligations and their distinctive features, including their links to the objectives of contestability and fairness. Third, attention turns to the two complementary pillars on which the implementation of the DMA relies on, namely compliance and public enforcement. Finally, other important topics such as the DMA's institutional set-up, private enforcement, the interplay of the DMA with other laws and future proofness of the DMA are examined.

## B. Gatekeeper designation

### B.1. Overview

The DMA's personal scope of application is determined by the notion of "gatekeeper." That notion is based on a combination of three criteria that an undertaking must fulfil to be deemed such a gatekeeper. First, it must have a significant impact on the internal market. Second, it must provide a digital service which (i) falls into one of the ten categories of CPSs listed in the DMA[288] and (ii) is an important gateway for business users to reach end users. Third, it must enjoy an entrenched and durable position, in its operations, either currently or foreseeably, in the near future. It is only in the presence of those cumulative criteria that the legislator considered that sufficiently serious concerns of contestability or unfair practices arise to justify the imposition of behavioural obligations on digital service providers.[289]

Importantly, however, undertakings meeting those criteria are not automatically deemed gatekeepers. A Commission designation decision is required to

[286] Rec. 15-21 DMA.

[287] Rec. 31 DMA. Examples include the Commission's decisions in cases AT.39740 *Google Search (Shopping)*, AT.40462/AT.40703 *Amazon Marketplace* and *BuyBox*, and AT.40437 *Apple – App Store Practices (Music Streaming).*

[288] Art. 2, point (2), DMA.

[289] Rec. 15 DMA.

this effect. Absent that, undertakings are not bound by any of the obligations laid down in the DMA. Consequently, enforcement of the DMA against them, whether by the Commission or by national courts, also cannot take place.

The crucial role of gatekeeper designation for the functioning of the DMA explains why designation is not framed as a discretionary power of the Commission, but as an obligation that arises whenever there is evidence that the relevant criteria are fulfilled.[290] The importance of gatekeeper designation and the ensuing need to ensure a fast and streamlined process[291] also explain the particular features of the designation mechanism. First, the DMA provides for a set of gatekeeper presumptions based on quantitative thresholds (essentially, the undertaking's annual EU turnover or market capitalisation, and the number of active end and business users of the CPS in the EU), which can only be rebutted in exceptional circumstances.[292] Second, undertakings meeting those thresholds are required to notify the Commission thereof within 2 months,[293] on pain of fines.[294] And third, the Commission is to designate those undertakings within 45 working days from a complete notification, unless it accepts (if appropriate, following a market investigation) that the undertakings have successfully rebutted the presumptions.[295]

While presumptions can lead to false positives (which is why the DMA contains a rebuttal mechanism), they can also lead to false negatives. To address that risk, the DMA provides for an alternative "qualitative" designation process based on a market investigation. This process is meant to enable the designation of those undertakings that do not satisfy (all) the quantitative thresholds but nevertheless fulfil the three substantive gatekeeper criteria set out above. The DMA includes a list of elements that the Commission may take into account in its assessment.[296]

Importantly, the gatekeeper designation, and thus the obligations laid down in the DMA, only apply in relation to those CPSs provided by the gatekeeper that are considered (whether based on the presumptions or on the qualitative criteria) to be important gateways for business users to reach end users and that are listed as such in the Commission's designation decision.[297] In practice, this means that undertakings can be (and indeed have been) designated as gatekeepers in relation to some of their CPSs but not others.[298]

---

[290] Art. 3(1) DMA, providing that "an undertaking *shall* be designated as a gatekeeper if […]" [emphasis added'.

[291] Rec. 16 DMA. See also Case T-1077/23, *Bytedance v. Commission*, EU:T:2024:478, para. 233 (appeal pending in C-627/24 P).

[292] Art. 3(2) and 3(5) DMA.

[293] Art. 3(3) DMA.

[294] Art. 30(3)(a) and (b) DMA.

[295] Art. 3(4) and (5) DMA.

[296] Art. 3(8) DMA and Rec. 24.

[297] Art. 3(9) and Rec. 15 and 29 DMA.

[298] However, it is noteworthy that certain obligations of the DMA pull within their orbit other CPSs or services of the gatekeeper.

To date, seven undertakings have been designated as gatekeepers, for a total of 24 CPSs.[299]

Given that it is at the same time a requirement for designation and the target of the DMA obligations, the notion of important gateway for business users to reach end users within the meaning of Article 3(1) DMA deserves particular attention. Two points bear emphasis.

First, the CPS must be an "important" gateway, not the *most important*, let alone the *only* gateway.[300] It follows from this that there can be several gatekeepers within the same CPS category, as the DMA explicitly recognises.[301] And indeed, the Commission has already designated several CPSs as important gateways within each CPS category.[302] This is not to say that a CPS's scale relative to other CPSs within the same CPS category is irrelevant as such to the notion of important gateway. Indeed, one of the elements that undertakings can rely on to try to rebut the presumption arising from the user thresholds is "the importance of the undertaking's core platform service considering the overall scale of activities of the respective core platform service."[303] However, it is not just because an undertaking's CPS is smaller than the CPS of a gatekeeper or that its position is contestable by gatekeepers that it cannot be a gatekeeper itself. This became clear in *Bytedance*, where the General Court rejected Bytedance's argument that the Commission should have concluded that TikTok's smaller scale compared with other online platforms meant that it could not be an important gateway.[304] This is one important element that distinguishes the notion of gatekeeper under the DMA from that of dominant position under Article 102 TFEU.

Second, the DMA's recitals mention a number of distinctive features of CPSs and gatekeepers, such as extreme scale economies, very strong network effects,

---

[299] Those are: (1) Alphabet's Google Search, YouTube, Google Maps, Google Play, Google Shopping, online ad services, Google Android and Google Chrome (see Commission decision C(2023) 6101 final of 5 September 2023); (2) Amazon's Marketplace and Amazon Advertising (see Commission decision C(2023) 6104 final of 5 September 2023); (3) Apple's App Store, Safari, iOS and iPadOS (see Commission decision C(2023) 6100 final of 5 September 2023, as amended by Commission decision C(2024) 2500 final of 29 April 2024); (4) Booking Holdings' Booking.com (see Commission decision C(2024) 3176 final of 13 May 2024); (5) ByteDance's TikTok (see Commission decision C(2023) 6102 final of 5 September 2023); (6) Meta's Facebook, Instagram, Marketplace, Whatsapp, Messenger and Meta Ads (see Commission decision C(2023) 6105 final of 5 September 2023); and (7) Microsoft's LinkedIn and Windows PC OS (see Commission decision C(2023) 6106 final of 5 September 2023). All designations are based on the application of the presumptions, but the one of Apple's iPadOS, which was of a qualitative mature.

[300] See also T-1077/23, *Bytedance v. Commission*, para. 210.

[301] Rec. 32 DMA.

[302] For instance, Facebook, Instagram, LinkedIn and TikTok, which belong to the category of online social networking services, have all been designated as CPSs constituting important gateways.

[303] Rec. 23 DMA.

[304] The General Court noted, *inter alia*, that TikTok's relative scale reached approximately half of the size of Facebook and of Instagram. This, so the Court held, distinguished TikTok's case from that of Microsoft's Bing and Edge, which were shown to be 10 or even 25 times smaller than other CPSs within their respective CPS categories. See T-1077/23, *Bytedance v. Commission*, para. 240.

lock-in effects, a lack of multi-homing, vertical integration and data driven-advantages.[305] However, those are mere examples rather than boxes to be ticked for a CPS to be considered an important gateway. This was once again confirmed by the General Court in *Bytedance*, when it rejected Bytedance's claim that the Commission should have accepted its rebuttal argument that TikTok is not an important gateway on the ground that a significant proportion of TikTok users multi-home.[306] After all, the fact that the features referred to in the DMA's recitals are not cumulative requirements for the notion of important gateway is rather intuitive, given that the DMA applies to a range of different categories of CPSs and that the presence of those features can vary greatly across CPS categories.[307]

In general, designation – even quantitative – is not always a straightforward exercise in practice. As shown by the designation decisions adopted so far, the Commission assesses thoroughly the information provided by the undertakings in their notification form (the "Form GD")[308] and, in several instances, the scope of its designation does not correspond to the narrative put forward by the undertakings in their notifications. Unsurprisingly given the high stakes of designation, three out of the seven designation decisions issued so far have led to actions for annulment by the respective gatekeepers,[309] and in one case even to an application for interim measures.[310] Litigation is also pending in relation to a decision *not* to designate a gatekeeper in relation to a given CPS.[311] So far, the most contentious issues in relation to designation have involved CPS delineation and attempts at rebutting the gatekeepers presumptions.[312] Those issues are examined in the next sections.

---

[305] Rec. 2, 3 and 13 DMA.

[306] T-1077/23, *Bytedance v. Commission*, paras. 175 and 182-214.

[307] E.g., end user multi-homing tends to be more common within some CPS categories (such as online social networking services and video-sharing platform services) than others (such as online search engines and web browsers). See also T-1077/23, *Bytedance v. Commission*, paras. 183-184.

[308] The template for the Form GD is attached as Annex I to Commission Implementing Regulation (EU) 2023/814 of 14 April 2023 on detailed arrangements for the conduct of certain proceedings by the Commission pursuant to Regulation (EU) 2022/1925 of the European Parliament and of the Council (OJ L 102, 17.4.2023, p. 6) (the "DMA Implementing Regulation").

[309] T-1077/23, *Bytedance v. Commission*; T-1078/23, *Meta v. Commission* (pending); and T-1080/23, *Apple v. Commission* (pending).

[310] Case T-1077/23 R, *Bytedance v. Commission*, EU:T:2024:94. The application for interim measures has been rejected.

[311] T-357/24, *Opera Norway v. Commission* (pending), which concerns the Commission decision not to designate Microsoft as a gatekeeper in relation to its web browser CPS Edge.

[312] Other issues include, e.g., the identification and calculation of end and business users for the purpose of determining whether the thresholds in Art. 3(2)(b) and (c) DMA are met, in light of the rules set out in the Annex to the DMA, or the qualification of a CPS as belonging to a particular category among those listed in Art. 2, point (2), DMA (which can be relevant, since some DMA obligations, such as Art. 6(12) DMA on fair access, only apply to certain categories of CPSs and not to others).

### B.2. Core platform services delineation

Firms active in the digital sector often do not just provide a single neatly delineated CPS, but several interrelated or integrated services or features, or even several versions of the same service. This means that the delineation of CPSs (i.e., the determination of their exact scope) and in particular whether or not they should be deemed to constitute a single or distinct CPSs, might not be clear-cut. The DMA does not contain detailed guidance on CPS delineation, besides some provisions in the Annex[313] and a prohibition on gatekeepers artificially segmenting their CPS as a way to circumvent designation.[314]

Yet, the stakes of CPS delineation can be high. First, delineation can determine whether or not a CPS meets the user thresholds for quantitative designation. In some cases, splitting CPSs may mean that some of them, if considered on their own, do not reach the quantitative thresholds for designation, whereas defining one single CPS may lead to the opposite result. Second, CPS delineation can determine whether a gatekeeper needs to comply with those DMA obligations that govern the relationship between *distinct* services of the same undertaking. Examples include Article 5(2) DMA, which prohibits *inter alia* the cross-use or combination of personal data from different CPSs or services of the gatekeeper absent end user consent, or Article 6(5) DMA, which prohibits favouring of the gatekeeper's own services in ranking. Considering two services as one single CPS means that those prohibitions will not apply between them.

Those issues have already arisen in concrete cases and even given rise to litigation.

For instance, when determining the CPSs in relation to which Apple had to be designated as gatekeeper, the Commission was faced with the question whether Apple's App Store constitutes a single CPS or ought to be split into distinct CPSs depending on the devices on which it is offered (e.g. iPhones, iPads, Mac computers). The Commission concluded, contrary to Apple's view, that the App Store constitutes a single online intermediation CPS, irrespective of the device. That finding was *inter alia* based on the observation that the App Store is used for the same purpose across all devices on which it is available, namely to intermediate the distribution of apps between business and end-users.[315] As a result, the Commission designated Apple as a gatekeeper in relation the App Store as a whole and not only in relation to the App Store on iOS (which, had

[313] DMA Annex, Sect. D.2.b.-c., essentially states that CPSs provided by the same undertaking shall be considered distinct for the purposes of calculating user numbers if: (i) the CPSs belong to different CPS categories pursuant to Art. 2, point (2), DMA; or (ii) the CPSs are used for different purposes by either their end users or their business users, or both. This applies even if the CPSs are offered in an integrated way or if their end or business users are the same.

[314] Art. 13(1) and Rec. 70 DMA.

[315] Commission decision C(2023) 6100 final of 5 September 2023, Section 5.1.1.2.

the App Store been split by device, would have been the only CPS to meet the user thresholds in Article 3(2)(b) DMA).[316] This finding has been challenged by Apple as part of its action for annulment of the Commission designation decision.[317]

A second example relates to the delineation of Meta's online social networking CPS Facebook. Meta claimed Facebook to be part of a single ad-supported online social networking CPS, comprising all features of Facebook (i.e., Messenger, Marketplace, Facebook Dating and Facebook Gaming Play) and Instagram, as well as Meta's online advertising services Meta Ads (or, alternatively, to be part of a single online social networking CPS, distinct from Meta Ads).[318] Contrary to Meta's view, the Commission concluded that Instagram was a distinct CPS from Facebook, *inter alia* since Meta offers those two services separately to end and business users.[319] Meta Ads was also considered to be distinct, *inter alia* since it belongs to a different CPS category from that of Facebook.[320] Likewise, the Commission found that Messenger and Marketplace should not be regarded as mere functionalities of Facebook, but as standalone CPSs, *inter alia* because they belong to different CPS categories from Facebook (respectively, number-independent interpersonal communication services and online intermediation services) and they were either developed as, or evolved into, separate services from the Facebook social network CPS.[321] Accordingly, the Commission's designation decision lists Facebook, Instagram, Meta Ads, Messenger and Marketplace as distinct CPSs.[322] This means that Article 5(2) DMA, and particularly the prohibition on user data combination, applies between those CPSs and between them and other services of Meta, with potentially substantial implications for Meta's business model, which relies on the accumulation and combination of user data to support its online advertising services.[323] Meta has challenged the Commission's designation decision on some of those points.[324]

---

[316] Ibidem, Art. 2.

[317] T-1080/23 *Apple v. Commission* (pending).

[318] Commission decision C(2023) 6105 final of 5 September 2023, Section 5.1.1.1.

[319] Ibidem, Section 5.1.1.2.2.

[320] Ibidem, Section 5.3.1.2.

[321] Ibidem, Sections 5.5.1.2 and 5.6.1.2. In addition, the Commission found that Facebook Dating and Facebook Gaming Play constitute distinct services from the Facebook online social networking CPS, since Meta offers them as a clearly identifiable and distinct services from that of Facebook and, in any event, those services fulfil specific and distinct purposes. Ibidem, Sections 5.1.1.2.3 and 5.1.1.2.4.

[322] Ibidem, Art. 2.

[323] The fact that Messenger is qualified as a number-independent interpersonal communication service ("NIICS") also entails that it is subject to the specific interoperability obligations laid down in Art. 7 DMA.

[324] T-1078/23, *Meta v. Commission* (pending).

### B.3. Rebutting the gatekeeper presumptions

As mentioned, to avoid designation, undertakings meeting the quantitative thresholds may submit, as part of their notification, arguments seeking to rebut the presumptions of gatekeeper status triggered by those quantitative thresholds.[325] The burden is thus on the undertaking concerned to adduce evidence rebutting the presumptions.

So far, most undertakings that notified the Commission that they met the quantitative thresholds also attempted to rebut the gatekeeper presumptions in relation to at least one of their CPSs. While the Commission accepted some rebuttals (in some cases, following a market investigation),[326] it rejected others,[327] which eventually led to litigation. The General Court's first judgment concerning the DMA, in *Bytedance*, focuses precisely on the framework applicable to rebuttals. It confirms that the possibility to rebut the gatekeeper presumptions is subject to strict requirements, in terms of substantive standard, standard of proof and procedural rules.[328]

As regards the substantive standard, undertakings must demonstrate that, exceptionally, although they meet the quantitative thresholds, due to the circumstances in which their CPS operates, they do not satisfy (at least one of) the qualitative requirements for gatekeeper designation laid down in Article 3(1) DMA. For the Commission to take them into account, the arguments should "directly relate to the quantitative criteria" laid down in Article 3(2) DMA.[329] This does not mean that arguments can be disregarded as irrelevant on the mere ground that they are not expressed in figures, but they must be specifically and concretely aimed at rebutting one of the three gatekeeper presumptions.[330] Moreover, given that, as explained above, the typical features of CPSs listed in the recitals of the DMA are not conditions *sine qua non* for a CPS to be regarded as an important gateway, the mere fact that a CPS does not display one of those features will not automatically be sufficient to rebut

[325] Art. 3(5) DMA. In this respect, the DMA differs from the DSA, which does not provide for this possibility.

[326] Rebuttals have been accepted in relation to: (1) Alphabet's Gmail (see Commission decision C(2023) 6101 final of 5 September 2023); (2) Microsoft's Outlook.com, Bing, Edge and Microsoft Advertising (see Commission decisions C(2023) 6106 final of 5 September 2023 and C(2024) 806 final of 12 February 2024); (3) Samsung's Internet Browser (see Commission decision C(2023) 6103 final of 5 September 2023); (4) Apple's iMessage (see Commission decision C(2024) 785 final of 12 February 2024); (5) ByteDance's TikTok Ads (see Commission decision C(2024) 3153 final of 13 May 2024); and (6) the Musk Group's X and X Ads (see Commission decisions C(2024) 3156 final of 13 May 2024 and of 16 October 2024).

[327] Rebuttals have been rejected in relation to Meta's Messenger and Marketplace and Bytedance's TikTok.

[328] T-1077/23, *Bytedance v. Commission*, para. 233.

[329] Rec. 23 DMA.

[330] T-1077/23, *Bytedance v. Commission*, paras. 47-48 and 326. All the more so, arguments that are not even related to the notion of gatekeeper cannot be accepted, such as justifications on economic grounds seeking to enter into market definition or to demonstrate efficiencies deriving from a specific type of behaviour. See Rec. 23 DMA and T-1077/23, *Bytedance v. Commission*, para. 46.

the presumption. Specific account should always be taken of the circumstances in which the relevant CPS operates.[331]

The standard of proof is also high, as the notifying undertaking's arguments must be "sufficiently substantiated" and they must "manifestly call into question the presumptions."[332] In other words, the arguments must be supported by evidence and capable of showing, with a high degree of plausibility, that the presumptions are called into question. Mere proof of the existence of doubts or *prima facie* evidence is not sufficient.[333]

In terms of procedural requirements, the evidence must be presented as part of the undertaking's notification and must clearly identify which of the three cumulative requirements set out in Article 3(1) DMA it relates to.[334] The undertaking will not be able to submit, for the first time before the General Court, rebuttal arguments which it had not submitted during the administrative procedure, unless it seeks to challenge a matter of law or of fact on which it was not able to comment during that procedure.[335]

If the rebuttal arguments meet the applicable criteria in terms of substance, standard of proof and procedure, the Commission is required to at least open a market investigation in order to test the undertaking's rebuttal arguments with relevant market players.[336] The Commission could, as an alternative, also directly accept the rebuttal arguments without launching a market investigation.[337] So far, it has done so when it found that the undertaking's arguments were not only sufficient to manifestly call into question the quantitative presumptions, but also clearly and comprehensively demonstrated that one or more of the requirements of Article 3(1) DMA was not fulfilled.[338]

## C. Substantive obligations

### C.1. Overview

The core provisions of the DMA are definitely its Articles 5, 6 and 7, which are intended to concretely achieve the DMA's contestability and fairness objectives. Those provisions contain closed lists of behavioural obligations applicable to gatekeepers, totalling 22 obligations and covering areas such as end-user and

[331] T-1077/23, *Bytedance v. Commission*, paras. 176-185. See also Section B.1 above.

[332] Art. 3(5) DMA.

[333] T-1077/23, *Bytedance v. Commission*, para. 71.

[334] Art. 3(5) DMA and Art. 2(3) DMA Implementing Regulation.

[335] T-1077/23, *Bytedance v. Commission*, para. 234.

[336] Art. 17(3) DMA. This is what the Commission did in relation to Microsoft's Edge, Bing and Advertising, Apple's iMessage and the Musk Group's X. In light of the outcome of the market investigation, the Commission then accepted the rebuttals.

[337] As the use of "may" in Art. 3(5), subpara. 3, DMA shows.

[338] That was the outcome in relation to e.g., Alphabet's Gmail, Microsoft's Outlook.com and Bytedance's TikTok Ads.

business-user data, mobile ecosystems, interoperability, fair access, transparency and commercial relationships with gatekeepers.[339] They are formulated either as positive obligations ("the gatekeeper shall…") or as prohibitions ("the gatekeeper shall not…").[340] While some obligations only apply to specifically identified categories of CPSs, others are meant to apply to any category.[341] Although they refer to a multitude of diverse behaviours and CPSs, the obligations laid down in Articles 5, 6 and 7 DMA share some key common features. First, they are all directly applicable and *ex ante* rules. Second, most (if not all) of them can be linked to both, and not only one, of the DMA's fundamental goals, namely contestability and fairness.

### C.2. Directly applicable and *ex ante* nature

*Direct applicability.* The DMA's behavioural obligations are grouped into different articles to distinguish those that are "susceptible of being further specified" by an *ad hoc* Commission decision concerning a particular gatekeeper (i.e., the obligations in Articles 6 and 7)[342] from those that are not susceptible of further specification, other than in the event of circumvention[343] (i.e., the obligations in Article 5).[344] On this basis, a common misconception is that the Articles 6 and 7 obligations would not be directly applicable. However, "susceptible" of further specification does not mean *requiring* further specification: it is apparent from the DMA that the Commission has discretion as to whether to provide further specification.[345] And the absence of a Commission specification decision does not exempt gatekeepers from the duty to comply with the obligations in Articles 6 and 7.[346] Accordingly, it also does not prevent the Commission from pursuing non-compliance proceedings and from imposing fines or periodic penalty payments.[347] At the time of writing, there are indeed three open proceedings for possible non-compliance with (not previously specified) Article 6 obligations.[348]

[339] In addition, the DMA also imposes some obligations on gatekeepers of a more procedural nature. See e.g., Art. 14 (information on concentrations) and Art. 15 (submission of an audit) DMA.

[340] See also Part I, Section D, above.

[341] See, as examples of the first type, Art. 6(3) DMA (uninstallation and change of default settings) and Art. 6(12) DMA (fair access); as examples of the second type, Art. 5(2) DMA (consent for personal data use) and Art. 6(2) DMA (no use of business user data).

[342] See Art. 8(2) DMA.

[343] Art. 8(2) and Rec. 65 DMA.

[344] Moreover, while Arts. 5 and 6 DMA cover various obligations concerning different CPSs, Art. 7 DMA is focused on the obligation to ensure interoperability between NIICSs. Since the text relating to that obligation (which was not in the original Commission proposal but was added at a later stage) spans over several paragraphs, those paragraphs were placed in a separate article.

[345] Art. 8(2) ("may"), Art. 8(3) ("shall have discretion") and Rec. 65 DMA.

[346] Art. 8(1) DMA.

[347] Art. 8(4) and Rec. 65 DMA.

[348] Cases DMA.100193 *Alphabet – Google Search* (Art. 6(5) DMA); DMA.100185 *Apple – iOS* (Art. 6(3) DMA); and DMA.100206 *Apple new business terms* (*inter alia* Art. 6(4) DMA).

*Ex ante nature*. The obligations in Articles 5, 6 and 7 DMA are intended to address those practices that the EU legislature identified as undermining contestability or fairness in the digital sector, or both, and as having a particularly negative direct impact on business users and end users.[349] However, while the design of the obligations was inspired by the DMA's objectives, their applicability is not subject to those practices actually affecting, or risking to affect, contestability or fairness in individual cases. Rather, the obligations in Articles 5, 6 and 7 are formulated as *ex ante* rules, which apply irrespective of actual of potential effects of the gatekeeper's conduct on contestability or fairness – in other words, as *per se* rules. Moreover, although some obligations leave room for gatekeepers to claim justifications, those are limited to integrity, security or privacy considerations and do not allow gatekeepers to claim countervailing efficiencies.[350] The *ex ante* nature of the DMA obligations is a key factor that distinguishes them from the prohibition on abuse of dominance under Article 102 TFEU. Indeed, a finding of abuse requires the capability of a given practice to produce anti-competitive effects and allows the dominant undertaking to escape such a finding by demonstrating objective justifications, including pro-competitive effects.[351]

That said, the DMA's contestability and fairness objectives can still play a concrete role in the practical implementation of the DMA, from at least two perspectives.

First, they can come into play in assessing whether the measures implemented by the gatekeeper effectively comply with the DMA obligations. Article 8(1) DMA requires those measures to "be effective in achieving the objectives of this Regulation and of the relevant obligation." Moreover, Article 13(4) DMA prohibits gatekeepers from engaging in "any behaviour that undermines effective compliance with the obligations of Articles 5, 6 and 7." In some cases, the requirement for effectiveness is even emphasised in the wording of the obligation itself.[352] The contestability and fairness objectives could thus play a concrete role in assessing gatekeepers' compliance with a given obligation where, although the measures implemented by the gatekeeper are on their face in line with a given obligation, there are doubts as to whether they effectively achieve the objectives of the obligation. This could be, for instance, because the scope of the measures is too limited, or because their benefits are jeopardised by other measures implemented by the gatekeeper.

Second, contestability and fairness are also intended to guide the Commission when it decides to specify the measures that a gatekeeper should implement to comply with the obligations in Articles 6 and 7 DMA (or even Article 5

[349] Rec. 31 DMA. The objective(s) pursued by a particular obligation is typically identified in the accompanying recitals, although some are more explicit than others.

[350] Arts. 6(4), 6(7) and 7 DMA. The measures should be duly justified by the gatekeeper and strictly necessary and proportionate to the relevant objectives.

[351] See, e.g., Case C-377/20, *Servizio Elettrico Nazionale and Others*, EU:C:2022:379, para. 103.

[352] E.g. Art. 6(4), 6(7), 6(9) DMA.

in case of possible circumvention). Article 8(7) DMA requires the Commission, in specifying the measures, to "ensure that the measures are effective in achieving the objectives of this Regulation and the relevant obligation."
Finally, the contestability and fairness objectives should also help identifying *other* practices in the digital sector that are not caught by Articles 5, 6 and 7 DMA but are nevertheless detrimental to those objectives. This can trigger a process governed by Article 19 DMA, possibly culminating in the addition of new obligations or in the update of existing obligations.

### C.3. Link to contestability and fairness

A closer look at the contestability and fairness objectives shows that they are conceived rather broadly under the DMA, which is reflected in the multitude, diversity and far-reaching scope of the obligations laid down in Articles 5, 6 and 7 DMA.
This is especially visible in relation to contestability. Under the DMA, pursuing contestability is not only about halting practices that can increase barriers to entry and expansion and thus undermine contestability, but also about mandating active behaviours by gatekeepers with a view to *lowering* existing barriers and thus positively promoting contestability.[353] The former aspect is typically rendered through negative obligations, the latter through positive obligations (e.g., the obligations mandating access).[354] Moreover, the objective of contestability relates not only to the gatekeeper's CPS listed in the designation decision that triggers the application of the particular obligation, but also to *other* digital services of the gatekeeper, such as those provided together with, or in support of, that CPS.[355] This is also in line with the DMA's clarification that contestability may justify creating or increasing *intra*-platform competition as a way to compensate for ineffective *inter*-platform competition.[356] In addition, practices are also deemed to limit contestability under the DMA where they prevent other operators from having the same access to a key input as the gatekeeper and are therefore capable of impeding innovation and limiting choice for business users and end users.[357]
Similarly, fairness encompasses *inter alia* the setting by gatekeepers of unbalanced conditions for the use of their CPSs or of related or supporting services that does not allow others to capture fully the benefits of their own contributions.[358] But it also relates to the exclusion or discrimination against business

[353] See Rec. 32 DMA.
[354] E.g., Art. 6(11) and (12) DMA.
[355] See, e.g., Rec. 31 (last sentence) and Art. 12(5)(a)(i) DMA. Relevant examples include the obligations against self-preferencing, discussed below.
[356] Rec. 32, last sentence, DMA.
[357] Art. 12(5)(a)(ii) DMA.
[358] Rec. 33 DMA.

users, in particular if they compete with the gatekeeper's services.[359] Moreover, although the emphasis is on unfairness towards business users, the DMA also contains several explicit references to the need to protect *end* users from unfair practices by gatekeepers that may affect them directly.[360]

The multi-faceted and broad nature of the contestability and fairness objectives explains why the DMA obligations very often display a direct link to both objectives or to several facets of those objectives.

In some cases, the two objectives are presented equally. For instance, some obligations are aimed at promoting both contestability of the gatekeeper's CPS (i.e., inter-platform contestability) and fairness to the benefit of business users. This is the case of the prohibition in Article 5(3) on price-parity clauses, which prevent business users from offering their products through their own online sales channels or third-party intermediation services at different terms than those offered through the gatekeeper's intermediation service. Such clauses are clearly at the same time unfair towards business users and detrimental to inter-platform contestability.[361] The same applies to Article 6(4), which mandates gatekeepers, *inter alia*, to allow the effective installation and use of third-party apps or app stores on hardware or operating systems of the gatekeeper. This provision is aimed both at promoting inter-platform contestability and at protecting business users (and end users) from unfair practices.[362]

In other cases, more emphasis is placed on one objective, but the other objective is also important. An example in point are the obligations banning self-preferencing, which typically concern situations where gatekeepers are vertically integrated or have a dual role. Those include Articles 6(2) (prohibiting the use of business users' data to compete with them), 6(3) (mandating the possibility of software un-installation and change in default settings), 6(5) (prohibiting the favouring of the gatekeeper's own services in ranking) and 6(7) (mandating interoperability with third-party hardware and software on equal conditions as those available to the gatekeeper). Those obligations are clearly designed to ensure fairness to the benefit of business users. However, they also aim to ensure contestability of digital services of the gatekeeper *other* than the CPS that is directly concerned by the obligation, which are typically those that the gatekeeper's behaviour seeks to favour.[363]

Conversely, the obligations involving end user data are principally aimed at remedying a lack of contestability of CPSs. Article 5(2) does so by subjecting personal data processing, combination, and cross-use by gatekeepers to end users giving their consent, after having being presented with the specific choice of a less personalised but equivalent alternative. This provision aims to counter data accumulation by gatekeepers, which can increase barriers to

[359] Rec. 33 DMA.
[360] See, e.g., Rec. 4, 7 and 13 DMA.
[361] Rec. 39 DMA.
[362] Rec. 50 DMA.
[363] Rec. 46, 49, 51-52 and 55-57, read in conjunction with Rec. 32-33 DMA.

entry, and ultimately to improve the contestability of CPSs relying on user data, such as online advertising services.[364] Similarly, Article 6(9) ensures that end users can effectively port their data, with a view to easing restrictions to switching and multi-homing and, as a result, improving the contestability of CPSs.[365] However, in pursuing contestability objectives, both provisions also ensure that end users are treated fairly by granting them control over their own data.

Finally, on a more general level, contestability and fairness are intertwined in a virtuous mutually reinforcing circle.[366] Strengthening contestability can indirectly limit the gatekeeper's ability or incentive to engage in unfair practices. *Vice versa*, freeing business users from unfair practices by gatekeepers can indirectly enable them to better challenge the gatekeeper's position. As a result, ultimately, all the DMA obligations could also be viewed as (indirectly) beneficial to both objectives.

## D. Compliance and public enforcement

### D.1. Overview

The DMA establishes a detailed framework to ensure the fulfilment of its substantive obligations.

One of the distinctive features of the DMA is that, unlike Articles 101-102 TFEU, it places *ex ante* compliance by gatekeepers rather than *ex post* enforcement by the Commission at the centre of this architecture. This is made possible precisely by the directly applicable and *per se* nature of the DMA's substantive obligations, as explained above. Compliance with those obligations is to be monitored by the Commission,[367] with interested third parties playing an important role in this respect. Moreover, as previously mentioned, some of those obligations can be specified in an *ad hoc* Commission decision. In that case, the measures set out in that decision add to the substantive obligations that the gatekeeper is required to comply with, and the Commission is expected to monitor compliance with those measures as well.[368]

It is only if pro-active compliance by gatekeepers fails or appears to fail that enforcement of the obligations by the Commission enters the scene. That is achieved through proceedings for non-compliance, which can lead to the imposition of fines and periodic penalty payments (including, as a last resort, remedies for systematic non-compliance).[369] The threat faced by gatekeepers

[364] Rec. 36-37 DMA.
[365] Rec. 59 DMA.
[366] See Rec. 34 DMA.
[367] Art. 26(1) DMA.
[368] Arts. 8(2) and 26(1) DMA, respectively.
[369] Of course, private enforcement is also possible. See Section F below.

of such proceedings and of the possible monetary sanctions and remedies can also act as an incentive to ensure compliance.

Accordingly, the effective implementation of the DMA can be seen as hinging on two complementary pillars: compliance (including the monitoring thereof) on the one hand, and enforcement, on the other. As explained below, those two pillars each rely on a number of specific tools and procedural phases to ensure that gatekeepers fulfil the obligations in Articles 5, 6 and 7 as effectively and as fast as possible.

### D.2. Compliance pillar

Gatekeepers are automatically required to implement measures to comply with the obligations in Articles 5, 6 and 7 DMA within six months after the relevant CPS has been listed in the Commission's designation decision.[370] The grant of suspensions, exemptions or (in the case of Article 7) postponements of this duty to comply are reserved for exceptional circumstances and are subject to proof by the gatekeeper that the relevant requirements are satisfied.[371] Likewise, the possibility for the Commission to declare some obligations as not applicable is limited to the case of designation of so-called emerging gatekeepers, namely undertakings that do not yet enjoy an entrenched and durable position but will foreseeably do so in the near future.[372]

As previously mentioned, compliance should be effective in light of the objectives of the DMA and of the specific obligation.[373] The DMA's preference is for the gatekeepers to ensure compliance by design, that is, to integrate the implementing measures as much as possible into the technological design they use.[374]

Besides ensuring compliance, gatekeepers are also required, first, to actively demonstrate such compliance to the Commission and third parties[375] and, second, to monitor their own continued compliance. The latter is to be achieved by introducing a "compliance function" composed of one or more

[370] Art. 3(10) DMA. For the six undertakings designated in September 2023, the deadline for compliance was therefore March 2024. For the seventh (Booking), it was November 2024.

[371] See, respectively, Arts. 9, 10 and 7(6) DMA, allowing the Commission, respectively, to suspend a particular obligation if compliance would endanger the economic viability of the gatekeeper's operations, to exempt the gatekeeper from a particular obligation on grounds of public health or public security and to extend the time limits for ensuring interoperability of NIICSs in certain cases. So far, the Commission has not granted any suspension or exemption. It has however extended Meta's time limit to ensure interoperability in relation to Facebook Messenger by six months pursuant to Art. 7(6) DMA. See Commission decision of 25 March 2024 in case DMA.100097.

[372] That declaration must be made in the relevant designation decision. See Art. 17(4) and Rec. 74 DMA.

[373] Art. 8(1) DMA. The onus is on the gatekeeper to ensure that the measures it implements comply with applicable law.

[374] Rec. 65 DMA.

[375] Art. 8(1) DMA.

compliance officers within the gatekeeper, which is independent from the operational functions of the gatekeeper.[376] The main tool for gatekeepers to demonstrate compliance with the DMA's substantial obligations is the report that they are required to submit to the Commission within 6 months after designation and to update thereafter at least annually, describing "in a detailed and transparent manner" the measures they have implemented to ensure compliance.[377] Gatekeepers are also required to publish a non-confidential version of their compliance report, which is also made available on the Commission's DMA website.[378]

In turn, the gatekeepers' periodic compliance reports are a critical tool for the Commission and third parties to review the gatekeeper's effective compliance with the DMA's obligations. This is apparent from the very detailed and comprehensive nature of the information required in the template published by the Commission for this purpose.[379]

The content of the compliance reports (or the possible gaps identified therein) and potential information submitted by third parties or national authorities about gatekeepers' behaviours[380] can also trigger additional follow-up measures on the part of the Commission.

Some of those follow-up measures are specifically foreseen by the DMA. They include, first, possible monitoring actions, such as measures ordering the gatekeeper to retain documents relevant to assess compliance.[381] This is a novel power that is not available under Regulation 1/2003 and is inspired by the preservation obligations that exist *inter alia* in the context of US antitrust investigations. The Commission has already made use of this power in relation to most of the gatekeepers by ordering them to retain documents relevant to the DMA obligations, so as to preserve available evidence for potential subsequent enforcement actions.[382] To assist it in monitoring compliance, the Commission may also decide to appoint independent external experts and auditors or officials from national competent authorities.[383]

Second, the Commission may, already at this monitoring stage, exercise its investigative powers, a possibility explicitly foreseen by Article 20(1) DMA.[384] Those investigative powers are largely modelled on those already provided for by Regulation 1/2003, consisting of the power to issue requests for information,

[376] Art. 28 DMA.

[377] Art. 11 DMA.

[378] See https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports

[379] See https://digital-markets-act.ec.europa.eu/document/download/904debdf-2eb3-469a-8bbc-e62e5e356fb1_en?filename=Article%2011%20DMA%20-%20Compliance%20Report%20Template%20Form.pdf

[380] Art. 27(1) DMA. On information submitted by third parties, see also Section D.3 below.

[381] See also Part I, Section F, above.

[382] See https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689

[383] Art. 26(2) DMA.

[384] The Commission made use of its investigative powers as early as on 25 March 2024. See https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689

carry out interviews and conduct inspections.[385] The main novel element in this respect is the power to require access to undertaking's data and algorithms and information about testing, as well as related explanations.[386]

In addition to the tools explicitly granted by the DMA, in practice, the Commission also makes use of additional tools to monitor and promote compliance. One of those is the organization of public workshops with interested stakeholders to elicit their views on the gatekeepers' proposed compliance solutions and to enable them to ask questions.[387] Another is the hosting of meetings with gatekeepers and interested third parties and, in general, the engagement in informal "regulatory dialogues" with gatekeepers to monitor compliance and, when necessary, encourage gatekeepers to improve their compliance solutions. Whether spontaneously or following the regulatory dialogues with the Commission, gatekeepers have already rolled out multiple changes to comply with those obligations.[388]

Another element worth mentioning in the context of the compliance pillar is the possible specification of the obligations laid down in Articles 6-7 DMA.[389] True, the opening of specification proceedings can be triggered by possible flaws or gaps identified in a gatekeeper's compliance report or even by indications that the gatekeeper is circumventing the DMA obligations,[390] which could in some cases also justify, as an alternative, the opening of non-compliance proceedings. However, even in those cases, the purpose of specification decisions is to clarify[391] what the gatekeeper should do to implement a particular obligation. It is not to take issue with, and sanction, the way the gatekeeper has implemented it.[392] The only "punitive" feature of specification proceedings which is evocative of non-compliance proceedings is the possibility for the Commission to directly back its specification decision by the threat of periodic penalty payments in case of non-compliance with it.[393] However, even then, the actual imposition of those payments requires further procedural steps and a separate decision.[394]

---

[385] See Arts. 21, 22 and 23 DMA, respectively.

[386] Art. 21(1) DMA, in the context of requests for information. See also Art. 23(2)(d), (3) and (4) DMA in the context of inspections.

[387] See https://digital-markets-act.ec.europa.eu/events/workshops_en, which also includes links to the recordings of the workshops held in 2024.

[388] See, e.g., https://developer.apple.com/support/dma-and-apps-in-the-eu#dev-qaa:~:text=To%20comply%20with%20the%20Digital%20Markets%20Act%2C (Apple), https://www.google.com/chrome/choicescreen/ (Alphabet), https://blogs.microsoft.com/eupolicy/2024/03/07/microsoft-dma-compliance-windows-linkedin/ (Microsoft).

[389] See Art. 8(2) DMA.

[390] Art. 13(7) DMA.

[391] Through a formal Commission decision addressed to the gatekeeper, rather than mere informal dialogues.

[392] Moreover, the purpose of specification is also not to modify the content of the obligations as such, but only to clarify the measures that the gatekeeper should take to effectively comply with those obligations.

[393] Art. 31(1)(a) DMA.

[394] Art. 31(2) DMA.

Thus, the key feature of the DMA's specification process, which also sets it apart from the non-compliance proceedings, is its regulatory as opposed to sanctioning function. The purpose of specification is to determine in a more granular manner what a particular gatekeeper should do to comply with a specific obligation, taking into account the specific circumstances of the gatekeeper and of its CPS. The guiding principles in this respect are the effectiveness in achieving the objectives of the DMA and of the particular obligation, and proportionality.[395]

The specification process can take place either following a reasoned request of the gatekeeper (based on a specific template)[396] or on the Commission's initiative. In any event, the Commission has discretion in deciding whether to engage in the process, provided it complies with the principles of equal treatment, proportionality and good administration.[397]

The regulatory function of the specification proceedings is reflected at several levels. First, once launched, the proceedings are subject to compulsory and particularly short time limits.[398] Second, the process is meant to rely on technical input and guidance from interested third parties (e.g., the beneficiaries of the measures) to help craft more effective measures. This is why the DMA requires the Commission, when it communicates its preliminary findings to the gatekeeper, to publish a non-confidential summary of the case and of the envisaged specification measures to enable those third parties to provide comments.[399] Third, specification decisions are not set in stone. Proceedings may be reopened, including in the event that the specification measures turn out not to be effective.[400]

The two ongoing specification processes to ensure interoperability with Apple's iOS and iPadOS pursuant to Article 6(7) DMA serve as a good illustration of the level of technicality and granularity that specification measures can reach.[401] They also provide a foretaste of the potentially significant benefits of

[395] Art. 8(7) DMA.

[396] See https://digital-markets-act.ec.europa.eu/document/download/b034f7c4-c877-420c-87fa-0e69f8aea522_en?filename=Article%208%283%29%20DMA%20Template%20%28request%20for%20specification%20dialogue%29_1.pdf

[397] Art. 8(3) DMA. See also Section C.2 above.

[398] The specification decision must be adopted within six months from the opening of proceedings and must be preceded by the communication to the gatekeeper of the Commission's preliminary findings. See Art. 8(2) and (5) DMA.

[399] Art. 8(6) DMA.

[400] Art. 8(9) DMA.

[401] The two specification processes aim to specify the measures that Apple should implement, respectively, (i) to ensure interoperability in relation to several iOS connectivity features, predominantly used for and by connected devices (e.g., notifications, automatic Wi-Fi connection, AirPlay, AirDrop, or automatic Bluetooth audio switching) and (ii) in relation to the request-based process developers need to go through to obtain interoperability with a specific iOS or iPadOS feature (e.g., increased upfront transparency of internal iOS and iPadOS features, timely communication and updates, fair and transparent handling of rejections and a more predictable timeline). See https://digital-markets-act.ec.europa.eu/dma100203-consultation-proposed-measures-interoperability-between-apples-ios-operating-system-and_en and https://digital-markets-act.ec.europa.eu/

the DMA's specification instrument in terms of delivering fast and effective solutions for business and end users of CPSs. Of course, those benefits assume that the gatekeeper complies with the measures set out in the specification decision.

As the above overview demonstrates, compliance is a key pillar of the DMA architecture and the DMA offers a range of tools to promote it. Gatekeepers' compliance with the DMA obligations can occur spontaneously, can be facilitated by regulatory dialogues or can follow formal specification decisions. In all cases, it generally translates into a fast implementation of the DMA obligations, often in cooperation with the gatekeeper itself and the beneficiaries of those obligations (thus increasing the chances that the solution will work in practice). If compliance is maintained over time, this makes it possible to avoid both the enforcement phase and the litigation before the EU Courts that typically follows. Admittedly, gatekeepers are still free to challenge specification decisions in Court if they are dissatisfied with the specification measures or if they wish to raise a plea of illegality of the relevant obligation under Article 277 TFEU. Still, the lack of financial sanctions and of a finding of non-compliance in the specification decision (which would otherwise facilitate follow-on damages actions before national courts) should in principle help mitigate the gatekeepers' incentive to engage in potentially prolonged litigation against the specification decision as such.

### D.3. Public enforcement pillar

Where there are indications that a gatekeeper may not comply with one or more of the obligations in Articles 5, 6 or 7 DMA, the Commission may decide to resort to non-compliance proceedings.

The structure of non-compliance proceedings and the rules applicable to them[402] are inspired to a large extent by the infringement proceedings in antitrust cases governed by Regulation 1/2003.[403] Non-compliance proceedings formally start with a Commission opening decision.[404] This is followed by the communication of preliminary findings (similar to the statement of objections in antitrust cases), after which the gatekeeper is entitled to submit observations and to have access to the Commission's file.[405] On this basis, the

dma100204-consultation-proposed-measures-requesting-interoperability-apples-ios-and-ipados-operating_en

[402] Those rules are set out in the DMA itself and in the DMA Implementing Regulation.

[403] This is the result of an intentional choice. See Part I, Section F, above. See also Impact Assessment Report accompanying the Commission's proposal for the DMA, SWD(2020) 363 final, Part 1/2, para. 159 (finding that "Regulation 1/2003 offers a well- known and legally sound model that can be replicated").

[404] Art. 20(1) DMA.

[405] Arts. 29(3) and 34 DMA. The DMA does not however provide for a right for the gatekeeper to develop its arguments at an oral hearing.

Commission may then adopt a decision finding that the gatekeeper does not comply with one or more of the obligations in Articles 5 to 7 and ordering it to cease and desist with the non-compliance.[406] In the same decision, the Commission may also impose fines on the gatekeeper of up to 10% of its worldwide turnover, as well as periodic penalty payments in order to compel it to comply with its decision.[407] Alternatively, the Commission may close the proceedings by decision, without finding non-compliance.[408] The DMA also provides for the possibility to impose interim measures in the context of non-compliance proceedings.[409] Throughout the proceedings, the Commission is entitled to exercise investigative powers that are also largely modelled on those of Regulation 1/2003.[410]

This symmetry between the DMA and the antitrust procedural rules is important for at least two reasons. First, it enables the Commission, when enforcing the DMA, to draw on the extensive experience gathered in applying the antitrust procedural rules over the past decades. Second, the significant body of case law developed around the procedural provisions of Regulation 1/2003 may in principle apply to the implementation of the DMA's procedural rules (subject to any adaptations that may be necessary in light of the differences between the two instruments).[411]

Despite the overall strong similarities, the DMA's rules governing non-compliance proceedings depart from Regulation 1/2003 in some notable respects. First, whereas antitrust proceedings are not subject to any deadlines, the DMA requires the Commission to "endeavour" to adopt its non-compliance decision within 12 months from the opening of proceedings.[412] This deadline reflects the legislator's attempt to avoid replicating in the DMA context the oft-criticised long duration of antitrust proceedings and to ensure that the non-compliant conduct is quickly brought to a halt. Even though it is only expressed in best-endeavours terms,[413] the 12-months deadline may have a concrete impact on the length and the outcome of non-compliance proceedings. In particular, it may help push gatekeepers to offer compliant solutions at an early stage, in the hope to persuade the Commission to close the proceedings without a finding of non-compliance and without a fine. As a matter of fact, several gatekeepers

[406] Art. 29(1)(a) and (5) DMA.

[407] Arts. 30(1)(a) and 31(1)(h) DMA.

[408] Art. 29(7) DMA.

[409] Art. 24 DMA.

[410] Arts. 21, 22 and 23 DMA. See also Section D.2 above.

[411] This was indirectly confirmed by the General Court's recent order in Case T-284/24, *Nuctech v Commission*, EU:T:2024:564, para. 35, concerning the Foreign Subsidies Regulation, another recent Regulation whose procedural provisions are also largely inspired by those of Regulation 1/2003 (Regulation (EU) 2022/2560 of the European Parliament and of the Council of 14 December 2022 on foreign subsidies distorting the internal market, OJ 2022 L 330, p. 1).

[412] Art. 29(2) DMA.

[413] Unlike the deadline for the adoption of specification decisions pursuant to Art. 8(2) DMA, which cannot be derogated. See Section D.2 above.

have implemented changes precisely following the opening of non-compliance proceedings or the issuance of preliminary findings.[414]

Second, the DMA, unlike Regulation 1/2003, does not provide for the possibility for third parties to submit formal complaints regarding alleged infringements of the substantive obligations. Although third parties (e.g., business and end users of CPSs) may "inform" the Commission about gatekeepers' practices falling under the DMA,[415] the DMA does not grant them a right to participate in the proceedings and does not require the Commission to formally reject their submission if it does not intend to act on it.[416] In any event, third parties can still play an important role by submitting valuable information to the Commission (including anonymously through the Commission's whistleblower tool)[417] or by providing input in response to a Commission consultation.[418]

Third, the DMA deviates from the traditional access to file procedure, which is based on the disclosure to the investigated undertaking of non-confidential versions of the documents that are part of the Commission's file. As already mentioned,[419] the DMA mainly relies on a novel mechanism that is centred on the use of "confidentiality rings." Where this mechanism applies, documents are to be disclosed, in principle in their full version, to the gatekeeper's external counsel (usually in a data room) rather than to the gatekeeper itself.[420]

Fourth, the DMA allows for the possibility of imposing higher fines, of up to 20% of the gatekeeper's worldwide turnover, in case of recidivism.[421] The DMA also specifically mentions "recurrence" among the factors that the Commission is required to take into account in fixing the amount of a fine, in addition to gravity and duration.[422] Subject to respecting those criteria, and absent guidelines on the setting of fines (such as those applicable to infringements of the competition rules), the Commission enjoys considerable leeway in deciding the methodology it wishes to follow to determine the amount of fines for non-compliance with the DMA.

Last but not least, while the DMA provides for the possibility of commitments and remedies, those are not part of the "standard" non-compliance proceed-

---

[414] E.g., this has been the case of Apple in relation to the non-compliance proceedings concerning Art. 6(3) DMA (https://developer.apple.com/support/browser-choice-screen/) and of Meta in relation to the non-compliance proceedings concerning Art. 5(2) DMA (https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/).

[415] Art. 27(1) DMA.

[416] Unlike under Arts. 6-8 Commission Regulation (EC) No 773/2004 of 7 April 2004 relating to the conduct of proceedings by the Commission pursuant to Articles 81 and 82 of the EC Treaty (OJ L 123, 27.4.2004, p. 18).

[417] See https://digital-markets-act.ec.europa.eu/whistleblower-tool_en

[418] Art. 29(4) DMA. Third parties also play a role in the procedures relating to systematic non-compliance and commitments, as explained further below.

[419] See Part I, Section F, above.

[420] Art. 34(4) DMA. See also Art. 8 DMA Implementing Regulation.

[421] Art. 30(2) DMA.

[422] Art. 30(4) DMA.

ings, but can come into play at a potential subsequent stage, which is that of "systematic non-compliance." Where the conditions for a finding of systematic non-compliance with the DMA obligations are met,[423] the DMA enables the Commission to impose on the gatekeeper any behavioural or structural remedies that are necessary and proportionate to ensure effective compliance with the DMA. Those remedies may even include, depending on the circumstances, a temporary ban on concentrations involving the relevant CPSs or services.[424] As in the case of specification proceedings, the Commission is required to consult third parties on the remedies that is considers imposing.[425] The gatekeeper may escape the imposition of remedies by offering commitments to ensure compliance with the relevant obligation(s), which the Commission may decide to make binding, following a public consultation.[426]

To date, the Commission has opened six non-compliance proceedings against three gatekeepers. One in relation to Meta concerning its so-called "Consent or Pay" advertising model, to the extent that it forces users to consent to the combination of their personal data and fails to provide them with a less personalised but equivalent version of Meta's social networks, contrary to Article 5(2) DMA. Two in relation to Alphabet, concerning respectively (i) its app store rules, to the extent that they restrict the app developers' ability to freely communicate and promote offers and directly conclude contracts with end users, contrary to Article 5(4) DMA; and (ii) its potential self-preferencing of Google's vertical search services over similar rival services in the display of Google search results, contrary to Article 6(5) DMA. And three in relation to Apple, concerning respectively (i) its app store rules, to the extent that they restrict the app developers' ability to freely communicate and promote offers and directly conclude contracts with end users, contrary to Article 5(4) DMA; (ii) the design, *inter alia*, of its web browser choice screen, to the extent that it prevents end users from effectively exercising their choice of services within the Apple ecosystem, contrary to Article 6(3) DMA; and (iii) its contractual requirements for developers, to the extent that they restrict the provision of alternative app stores or the possibility to offer an app via an alternative distribution channel, contrary *inter alia* to Article 6(4) DMA.

## E. Institutional set-up

The core competencies under the DMA – designation of gatekeepers, specification and public enforcement of the obligations – are reserved for the Commission only, as the sole enforcer of the DMA.[427] Underlying this centralised

[423] Art. 18(1) and (3) and Rec. 75 DMA.
[424] Art. 18(1) and (2) and Rec. 75 DMA.
[425] Art. 18(5) DMA.
[426] Arts. 25, 18(6) and Rec. 76 DMA.
[427] Art. 38(7) and Rec. 91 DMA.

approach is the need to avoid the risk of regulatory fragmentation, given the pan-European reach of the addressees of the DMA's obligations.[428]

Despite calls by the Member States' national competition authorities ("NCAs") during the legislative process to provide for a joint application of the DMA by the Commission and NCAs,[429] NCAs do not have full-fledged enforcement powers under the DMA. They are however tasked with cooperating with and supporting the Commission in its enforcement, notably by assisting it in its market investigations, transferring to the Commission information they may receive from third parties on possible non-compliance and replying to Commission requests for information.[430] Where empowered to do so under national law, NCAs may also investigate on their own initiative possible cases of non-compliance by gatekeepers with the DMA substantive obligations on their territories, unless and until the Commission decides to open proceedings.[431]

This Commission-centric system of implementation of the DMA contrasts with the decentralised system of enforcement of Articles 101 and 102 TFEU, which relies on parallel enforcement by the Commission and NCAs. Since the DMA is without prejudice to the EU and national competition rules (as Article 1(6) DMA makes clear), NCAs will in principle still be able to intervene under those rules against unilateral conduct by gatekeepers that could also fall within the scope of the DMA. Indeed, the DMA does not provide for any mechanism similar to that of Article 11(6) of Regulation 1/2003, which would enable the Commission to relieve the NCAs of their competence to apply the competition rules in cases covered by the DMA. Still, the DMA prevents NCAs (and national authorities in general) from intervening when their decisions would run counter to decisions adopted by the Commission under the DMA.[432] It also includes detailed provisions governing the coordination between the Commission and NCAs in relation to their enforcement of the DMA and of the competition rules, respectively.[433]

In addition, the DMA also entrusts two distinct entities with the task of assisting the Commission in its enforcement. First, the High-Level Group for the DMA, which is composed of representatives of European bodies and networks and is intended to provide advice to the Commission in the areas of competence of its members, including on possible interactions between the DMA and the sector-specific rules.[434] Second, the Digital Markets Advisory

[428] Commission proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector, Explanatory memorandum, Section 3.

[429] See e.g., Joint paper of the heads of the NCAs of the EU, 'How national competition agencies can strengthen the DMA,' 22 June 2021, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Others/DMA_ECN_Paper.pdf?__blob=publicationFile&v=2

[430] Arts. 16(5), 38(6), 27(3) and 21(5) DMA.

[431] Art. 38(7) DMA.

[432] Art. 1(7) DMA.

[433] Art. 38(1) to (5) DMA.

[434] Art. 40 DMA and Commission Decision C(2023) 1833 final of 23 March 2023.

Committee, which is composed of representatives of Member States and is to be consulted by the Commission before adopting implementing acts under the DMA.[435]

Finally, public enforcement of the DMA by the Commission is meant to be complemented by private enforcement by the national courts of the Member States.[436] For this purpose, the DMA contains specific provisions regulating cooperation between the Commission and national courts aimed to ensure the uniform enforcement of the DMA.[437]

## F. Private enforcement

The DMA does not contain a specific provision enabling users to enforce its obligations against gatekeepers before national courts.[438] Nevertheless, the possibility of private enforcement is implicit in the DMA's provisions governing cooperation between the Commission and national courts.[439] It is also borne out by the DMA's reference to the Representative Actions Directive as being applicable to the representative actions brought against infringements by gatekeepers of the DMA that harm or may harm the collective interests of consumers.[440] In any event, the possibility of private enforcement of the DMA follows in principle from its directly applicable nature as a Regulation. As a result, business and end users should, where the relevant conditions are met, be able to rely on the DMA's substantive obligations before national courts against undertakings that have been designated as gatekeepers.[441]

In terms of types of private enforcement actions available, those should include, in particular, damages claims[442] and private injunctions. Moreover, both follow-on actions (based on a prior Commission decision finding non-compliance) and standalone actions (where no prior Commission non-compliance decision has been adopted) can be envisaged. In any event, national courts may not adopt decisions running counter to decisions that the Commission has adopted under the DMA (whether concerning non-compliance or for instance, specification) or that the Commission is contemplating in proceedings it has initiated under the DMA.[443]

---

[435] Art. 50 and Rec. 99-101 DMA.

[436] See Section F below.

[437] Art. 39 and Rec. 92 DMA.

[438] Unlike the DSA, whose Art. 54 specifically refers to damages actions. See Part II, Section D.1, above.

[439] Art. 39 and Rec. 92 DMA. See also Section E above.

[440] Art. 42 and Rec. 104 DMA.

[441] Absent prior designation, undertakings are not bound by the obligations and private enforcement is therefore excluded. See Section B.1 above.

[442] While the Competition Damages Directive does not apply to actions under the DMA, nothing would prevent Member States from extending their national measures transposing the Directive to damages claims based on the DMA.

[443] Art. 39(5) DMA.

While private enforcement of the DMA by national courts is still at its early stages, it has the potential to significantly enhance the effectiveness of the DMA's substantive obligations. Over time, it could thus become an important complement to the Commission's public enforcement. Moreover, the very risk of having to pay large amounts to compensate damages from DMA infringements may in itself contribute to increasing deterrence and ultimately fostering compliance by gatekeepers.

## G. Interplay with other laws

While the DMA lays down a comprehensive framework of substantive and procedural rules aimed at ensuring contestable and fair digital markets, it does not operate in a vacuum.

On the one hand, the DMA relies to a significant extent on external legal instruments. Examples include DMA's definitions of the CPS categories (many of which refer to the P2B Regulation or to certain Directives),[444] the notion of turnover for the purposes of the gatekeeper presumption (which refers to the Merger Regulation)[445] and the notion of user consent under Article 5(2) (which refers to the GDPR). Also, as mentioned above, the procedural rules governing the DMA's enforcement are largely modelled on Regulation 1/2003 (and are now in common with those of the DSA and the Foreign Subsidies Regulation), meaning that the body of related case law could be considered to apply *mutatis mutandis*. In addition, the Commission is to draw on the enforcement of Articles 101 and 102 TFEU when assessing possible extensions of the scope of the DMA to new practices or new CPSs[446] (just as past antitrust decisions have inspired many of the existing DMA obligations). On the other hand, the DMA may also contribute to the implementation of other laws. One example is the obligation on gatekeepers to submit to the Commission an audit of their user profiling techniques, which is then transmitted by the Commission to the European Data Protection Board to inform the enforcement of EU data protection rules.[447] Likewise, gatekeepers are required to inform the Commission of intended concentrations, which enables NCAs to use that information for national merger control purposes or to refer a transaction to the Commission under the Merger Regulation.[448] The DMA obligations themselves (or, more precisely, their role in constraining gatekeepers' conduct), can even have a direct impact on the Commission's review of concentrations involving gatekeepers under the Merger Regulation. A concrete example is the Commission's investigation into Amazon's proposed acquisition of iRobot,

[444] Art. 2, points (5), (6), (8), (9) and (13), DMA.
[445] Art. 3(2)(a) DMA (see Art. 2, point (30), DMA).
[446] Art. 19(1), last sentence, DMA.
[447] Art. 15 and Rec. 72 DMA.
[448] Art. 14 and Rec. 71 DMA.

which took into account the impact of the prohibition on self-preferencing in Article 6(5) DMA in assessing Amazon's incentives to foreclose rivals post-merger.[449] Finally, some of the novel procedural provisions of the DMA (for instance, as regards access to file based on mandatory confidentiality rings) are likely to inform the future revision of the antitrust procedural rules.[450]

The above are all examples of direct touchpoints between the DMA and other laws, where the two may influence one another in their implementation.

In addition, questions may (and in all likelihood, will) also arise as to the possible parallel application of the DMA and complementary regimes.[451] Those include not least the EU and national competition rules, which, as explained above, may catch conduct that is also prohibited under the DMA.[452] In this connection, one question that is likely to generate significant discussions in light of Article 1(5) and (6) DMA is the exact scope left by the DMA for the application of national obligations to gatekeepers.[453] A fine line might need to be drawn depending on the nature and purpose of the national rules at issue (e.g., whether or not they qualify as "competition rules" under Article 1(6) DMA) and the nature of the obligations imposed in the concrete case (e.g., whether they genuinely amount to "further," as opposed to stricter, obligations under Article 1(6)(b) DMA). In addition, complementary regimes also include other legal instruments which gatekeepers have to comply with, such as the GDPR, rules on consumer protection, product safety[454] and other EU legislation regulating the provision of digital services in the EU.[455] To the extent that some of those legal instruments may be enforced by national authorities, the DMA requires them and the Commission to cooperate with each other and coordinate their enforcement actions.[456]

## H. Future proofness

As explained, the DMA establishes a closed catalogue of clearly predefined *ex ante* obligations. Those obligations have a circumscribed material and personal

[449] M.10920 *Amazon/iRobot*. See European Commission's Competition Merger Brief, Issue 2/2024, p. 8.

[450] Commission Staff Working Document, SWD(2024) 216 final, Evaluation of Regulations 1/2003 and 773/2004, pp. 145–146.

[451] See also Part I, Section G, above.

[452] See Section E above.

[453] Art. 1(5) DMA prohibits Member States from imposing "further obligations" on gatekeepers "for the purpose of ensuring contestable and fair markets," but, at the same time, does not preclude them from imposing obligations on undertakings for matters falling outside the scope of the DMA, provided that they do not result from the status of gatekeeper. In stating that the DMA is without prejudice to national competition rules, Art. 1(6) DMA also includes in that notion "national competition rules prohibiting other forms of unilateral conduct insofar as they […] amount to the imposition of further obligations on gatekeepers."

[454] Art. 8(1) DMA.

[455] See Part I, Section G, above.

[456] Art. 37(1) DMA.

scope of application, namely undertakings which provide one or more services out of a closed list of CPS categories and which satisfy a set of clear quantitative criteria, or, alternatively certain qualitative criteria.

Such a closed set of rules (where the only element of openness comes from the qualitative designation tool) is clearly beneficial to legal certainty, predictability and fast implementation. However, it can come at the expense of flexibility and adaptability to future market developments, which are particularly likely in the digital sector given its fast-moving pace.

To remedy this, the DMA provides for a number of mechanisms meant to ensure its future proofness.

First, the DMA enables the Commission to conduct a market investigation to examine whether new CPS categories should be added to the list in Article 2, point (2), DMA. The findings of the market investigation shall be published in a report, which, where appropriate, can be accompanied by a legislative proposal to amend the DMA accordingly.[457]

Second, the Commission is required to examine at least every year whether new undertakings providing CPSs satisfy the qualitative requirements for gatekeeper status. It is also expected to review at least every three years whether designated gatekeepers continue to satisfy the requirements for designation and whether the list set out in the designation decisions of CPSs that constitute an important gateway is up-to-date. Where appropriate, those reviews should lead to amendments of the designation decisions[458] (which, in the case of qualitative designations, require a prior market investigation).

Third, the DMA also provides for the possibility to supplement or update the behavioural obligations in Articles 5-7 DMA to take into account further practices that limit contestability or fairness, including in light of the experience gathered through antitrust enforcement. Where there is a need to add entirely *new* obligations, the procedure to be followed is the same as that applicable to the addition of new CPS categories (i.e., a market investigation followed by a legislative proposal).[459] On the contrary, where all is required is to update *existing* obligations (e.g., by extending their scope to further CPS categories or by specifying them *erga omnes*), the Commission may directly proceed by means of a delegated act (following, once again, a market investigation).[460]

As follows from the above, the key tool to ensure future proofness of the DMA is that of market investigations, which are aimed to guarantee that any changes to the DMA's scope or obligations benefit from a solid evidentiary basis.[461]

---

[457] Art. 19(1) and (3)(a) DMA. The legislative proposal may also propose to remove existing CPS categories.

[458] Art. 4(2) DMA. Amendments are also possible on an *ad hoc* basis (see Art. 4(1) DMA).

[459] Art. 19(1) and (3)(a) DMA. The legislative proposal may also propose to remove existing obligations.

[460] Arts. 12 and 19(3)(b) DMA.

[461] See also Rec. 77 DMA.

The opening of market investigations can also be formally requested by Member States, which triggers a four-months period within which the Commission is required to assess whether such opening is justified.[462]

Finally, the DMA requires the Commission to publish an annual report on the implementation of the DMA and the progress made toward achieving its contestability and fairness objectives.[463] The Commission is also required to carry out an evaluation of the DMA every three years to assess whether the contestability and fairness objectives have been achieved and the impact of the DMA on business users and end users. The evaluations should also establish whether there is a need to amend the applicable rules, including as regards the lists of CPSs and substantive obligations.[464] The first evaluation report is due by 3 May 2026. This will allow for a first comprehensive stock-taking of the effectiveness of the DMA in achieving contestable and fair markets in the digital sector across the EU, to the benefit of business users and end users.

[462] Art. 41(1) and (3)-(5) DMA. In addition, Member States may also request the Commission to open a market investigation into possible systematic non-compliance by a gatekeeper with the DMA's substantive obligations (see Art. 41(2) DMA).

[463] Art. 35 DMA. Published reports are available at https://digital-markets-act.ec.europa.eu/about-dma/dma-annual-reports_en

[464] Art. 53 DMA.