IS THERE ANYTHING NEW UNDER THE SUN? A GLANCE AT THE DIGITAL SERVICES ACT AND THE DIGITAL MARKETS ACT FROM THE PERSPECTIVE OF DIGITALISATION IN THE EU[1]

Balázs Hohmann[*] and Bence Kis Kelemen[**]

Abstract: The adoption of the Digital Services Act (DSA) and Digital Markets Act (DMA) has been a great step towards regulating digital space and industry. The two regulations set out a comprehensive and long-awaited set of requirements for companies providing intermediary and gatekeeping services. According to some commentators, the new laws will largely redefine the operating conditions for businesses in the digital sector.

This article highlights key provisions of the DSA and DMA that may influence the evolution of the digital sector in Europe and shows that the DSA relies heavily on its predecessor, the e-Commerce Directive, and both regulations draw inspiration from other new-age EU secondary legislation, such as the General Data Protection Regulation (GDPR) and industry best practices.

The main conclusions of the article are the following: the changes can be considered a significant step forward from a regulatory perspective, but 'there is nothing new under the sun'. In other words, the regulations do not fundamentally change the liability regime of intermediary service providers, but rather take a necessary step forward to further regulate these businesses. Albeit the DSA and the DMA should be praised for their layered approach on allocating different responsibilities on different size undertakings – unlike the GDPR – as the main 'targets' of the regulations are primarily US-based big tech companies. It is still worrying that the DSA could also increase operational costs for European startups, potentially turning them away from the continent, which in turn could produce an innovation-cooling effect in the Union.

Keywords: DSA, DMA, intermediary services, gatekeepers, innovation

---

[1] Supported by the Hungarian Ministry of Justice to improve the quality of legal education.
DOI: 10.3935/cyelp.19.2023.542.

[*] Senior lecturer, University of Pécs Faculty of Law. Board member, Conciliation Board of Baranya County (Hungary).

[**] Senior lecturer, University of Pécs Faculty of Law. Associate, Környei Mátyás Law Firm.

1 Introduction

The European Parliament and Council adopted the Digital Services Act[2] (DSA) and the Digital Markets Act[3] (DMA) both based on Article 114 of the Treaty on the Functioning of the European Union (TFEU) in 2022. This marks another milestone on the European Union's route towards digitalisation and the regulation of big tech companies, furthermore giving birth to 'European digital constitutionalism', which can be characterised as a set of rules shielding individuals from abuse of power in the digital environment.[4] This route has been marked with other secondary EU legislation in recent years, such as the General Data Protection Regulation,[5] the AI Act[6] and the Cyber Security (NIS 2) Directive.[7] References can also be made to other secondary EU legislation that have entered the legislative process, such as the European Media Freedom Act,[8] the Cybersecurity Regulation,[9] the Information Security Regulation,[10] the Cyber Resilience Act,[11] and the Cyber Solidarity Act.[12] These pieces of secondary legislation – usually – create obligations for big tech companies that can be characterised as flagships of digitalisation and technological

---

2 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277 (DSA).

3 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265.

4 Maria Luisa Chiarella, 'Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment' [2023] Athens Journal of Law 33, 51.

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119 (GDPR).

6 The AI Act is now in the process of formal approval by the European Parliament and the Council after a political agreement on 9 December 2023 < https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473> accessed 12 December 2023.

7 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L333.

8 Proposal for a Regulation of the European Parliament and the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU 2022/0277(COD).

9 Proposal for a Regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (2022/0085 (COD).

10 Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union 2022/0084 (COD).

11 Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 2022/0272 (COD).

12 Proposal for a Regulation of the European Parliament and of the Council on laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity incidents 2023/0109 (COD).

development. Among these, the DSA and the DMA were set out to regulate intermediary service providers and gatekeepers, which are in the centre of the Digital Single Market.[13] The DSA – following of the logic of its predecessor, the e-Commerce Directive[14] – supplements the previous conditional liability regime applicable to intermediary service providers and gatekeepers with due diligence obligations and a framework for enforcing the legislation. The regulation takes a layered approach, that is to say, it differentiates between different types of service providers, which goes to the heart of the issue, distinguishing between 'regular' intermediary services and online platforms, search engines, and other gatekeeper-type companies. In comparison, the DMA sets out the requirements applicable to companies providing gatekeeping services, defining the criteria for designation as a gatekeeper, addresses unfair practices by gatekeepers, the specific requirements for certain gatekeeping services, and the enforcement rules for non-compliance. These rules can be seen as a gap-filling exercise, as there was no comprehensive regulation of gatekeepers in this form in the EU before.

Since some commentators argue that the DSA and the DMA will bring fundamental changes to the EU's digital regulatory environment,[15] the aim and goal of this paper is to scale back somewhat the expectations from these regulations. Therefore, the article will, first and foremost, introduce the reader to the DSA and the DMA, outlining their most important norms, and pointing out that 'there is nothing new under the sun'. Of course, it would not be fair to present the DSA and the DMA this way, since they indeed create new obligations for intermediary service providers and gatekeepers. Transparency obligations in the DSA for instance – although common in practice – come as a novelty in terms of legal obligations, and some important changes have also been made to the fundamentals of the enforcement mechanism adopted in the GDPR, for example in connection with the role of the European Commission. All in all, the argument advanced in this chapter is that the DSA and the DMA do not modify the cornerstone rules of intermediary liability, and therefore the fundamentals of the system remain unaffected and the regulatory methods used for creating additional layers to the regulations by the European Union cannot be considered a novelty, in the purest sense of the word, since other new-wave secondary legislation follows the same

[13] 'A Digital Single Market is one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence.' See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe COM(2015) 192, 3

[14] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L178 (e-Commerce Directive).

[15] Bissera Zankova, Gergely Gosztonyi, 'Quo vadis, European Union's New Digital Regulatory Package?' [2021] Бизнес и право 67, 70.

logical structure and methods. For example, the DSA does not change the fundamental liability system of intermediary service providers, but rather gives extra obligations for these service providers, and, what is also important, these two new regulations essentially follow in the footsteps of previous EU legislation mentioned above, such as the GDPR, in terms of the regulatory logic and methods. It needs to be noted, however, that according to one scholar, the DSA specifically addresses some of the deficiencies of the e-Commerce directive, for instance fragmentation regarding complementary norms and the application of the directive, and the discretion given to service providers when it comes to content moderation,[16] which is, of course, a welcome development in the field.

Another objective of the article is to analyse how the more robust, and stricter obligations placed on these service providers influence innovation in the field of digitalisation. The European Commission stated in the explanatory memorandum of the proposal for the DSA that supervising digital services will enhance innovation and growth in the single market.[17] Furthermore, in the eyes of the Commission, by harmonising obligations, the DSA might contribute to innovation by cutting compliance costs and it might also support growth in turnover in cross-border digital trade to the extent of EUR 8.6 billion to EUR 15.5 billion.[18] While agreeing with the Commission on the benefits of de-fragmentation of laws in this context, our conclusion in this regard is that such legislation can still increase operational costs for companies in Europe and/or targeting Europe as a market, which might bring European consumers into a more disadvantageous position, in contrast with the rest of the world, or it can possibly have an innovation-cooling effect, or, in other words, digital service startups might choose other States, for instance the US, to start and establish their business. This, in turn can seriously jeopardise the objective of both the DSA and DMA, namely the development of the Digital Single Market. By comparison, the DMA's explanatory memorandum argues that small and medium-sized enterprises operating in the European Union are unlikely to be designated as gatekeeper businesses under the new regulation.[19] They will therefore not be burdened with compliance costs that would put them at a competitive disadvantage. In the memorandum, the Commission expects to generate EUR 13 billion in additional consumer surplus linked to innovation by EU-based businesses.[20] Since only the largest operators are considered to be gatekeeping services, we can agree with this objective by looking at the DMA itself.

---

[16] Berrak Genç-Gelgeç, 'Regulating Digital Platforms: Will the DSA Correct Its Predecessor's Deficiencies?' (2022) 18 CYELP 25, 57-60

[17] 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. Explanatory Memorandum COM(2020) 825 final 6.

[18] ibid 11-12.

[19] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)' (Explanatory memorandum) COM/2020/842 final 13.

[20] ibid 10.

Since the DSA became applicable to very large online platforms (VLOPs) and very large online search engines (VLOSEs) on 25 August 2023, and the DMA entered into force on 25 June 2023, this creates ample opportunity to analyse the two above-mentioned new regulations.[21] To achieve this aim, the article will first provide an overview of the DSA, pointing out parallels with previous, existing, or even planned EU legislation (Part 2); second, it turns to the DMA with the same methodology (Part 3); and finally it offers conclusions based on the review of these new EU regulations (Part 4).

2 The Digital Services Act

The DSA consists of five chapters and 156 recitals. As Article 1 para 1 clearly states, the aim and goal of the regulation is to set harmonised rules – hence the regulation format – for a safe, predictable and trusted online environment that is compatible with fundamental rights and innovation alike.[22]

The DSA sets its scope to apply to intermediary services, but only those which are received by persons located in the EU or those who have their place of establishment in the Union. It is immaterial whether the intermediary service provider has a place of establishment in the EU or not.[23] According to one commentator, this rule in particular aims at taking back digital sovereignty for the EU and to push back against US-based companies dominating the market.[24] In our understanding, it also fits neatly into the so-called 'Brussels effect'. This phenomenon can be characterised as the unilateral ability of the European Union to regulate the global marketplace, as both participants of the market and other State actors align with existing EU legislation.[25] One commentator – supporting this position – claims that by adopting the DSA, the European Union can strongly influence how social media platforms moderate their content even globally.[26] According to that author, a similar example of the Brussels effect can be found in the EU Code of Conduct on Countering Illegal Hate Speech Online.[27] This latter document can be seen as

[21] ' Digital Services Act Takes Effect for Large Online Platforms' (*European Data*, 25 August 2023) <https://data.europa.eu/en/news-events/news/digital-services-act-takes-effect-large-online-platforms> accessed 30 August 2023; DMA Article 54.

[22] DSA, Article 1 para 1.

[23] DSA, Article 2 para 1.

[24] Gabi Schlag, 'European Union's Regulating of Social Media: A Discourse Analysis of the Digital Services Act' [2023] Politics and Governance 1, 2.

[25] Anu Bradford, *The Brussels Effect. How the European Union Rules the World* (OUP 2020) 1.

[26] Dawn Carla Nunziato, 'The Digital Services Act and the Brussels Effect on Platform Content Moderation' [2023] Chicago Journal of International Law 115, 117.

[27] ibid 120-121.

one of the predecessors of the DSA,[28] as it, in a non-binding form, contains rules for example regarding the review of notification of illegal hate speech.[29] Another example to illustrate this trend can be found in the GDPR, which sets its own territorial scope beyond those data controllers who are established in the EU to those who are not, but they still offer services in the Union.[30] The interpretation of the GDPR leads to similar results. For example, in the *Google v CNIL* case, the Court of Justice of the EU (CJEU) ruled that although the GDPR does not require controllers to apply the right to be forgotten globally – in that case Google, a search engine, to delete a certain link – supervisory authorities have the right to create global obligations.[31] Furthermore, the Brussels effect has already manifested itself in the area regulated by the DSA, namely intermediary service provider liability. The CJEU, in *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, determined that based on the e-Commerce Directive, Member State authorities have the power to oblige service providers – in that case Facebook – to take down illegal content globally.[32] This was reinforced by the above-mentioned extra territorial rule of the DSA. Turning back to the original point, the DSA applies to intermediary service providers, which play an important role in the EU's economy as well as in the daily life of Union citizens, but at the same time pose risks and challenges for users of these service as a result of digitalisation or digital transformation.[33]

Intermediary services are information society services as defined by Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015[34] – in other words, any services that are normally provided in exchange for renumeration, at a distance and by electronic means, and, as the last element of the definition, at the request of the recipient of the service itself[35] – laying down a procedure for the provision of information in the field of technical regulations and of rules on information society services. Nevertheless, the DSA limits its application

---

[28] There are other instruments and organisations that paved the way for the adoption of the DSA, such as the East StratCom Task Force, against Russian disinformation, the Resolution on Online Platforms and the Digital Single Market and the EU Code of Practice on Disinformation and Action Plan. See Schlag (n 24) 4.

[29] The EU Code of Conduct on countering illegal hate speech online. <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en> accessed 23 August 2023.

[30] GDPR, Article 3 paras 1-2.

[31] Case C-507/03 *Google v CNIL* ECLI:EU:C:2019:15, paras 64 and 72.

[32] Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* ECLI:EU:C:2019:821, paras 49-51.

[33] DSA, Recital 1.

[34] DSA, Article 3(g).

[35] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L241, Article 1(1)(b).

to 'mere conduit',[36] 'caching',[37] and 'hosting' services.[38] So far, these notions are almost identical to those of the e-Commerce Directive.[39] There are, however, two 'new' forms of intermediary services introduced by the DSA in comparison with the e-Commerce Directive, namely online platforms[40] and online search engines.[41] To name but a few examples for each services, 'mere conduit' and 'caching' services are internet services, direct messaging services (eg Viber), while 'hosting' services include online media sharing (eg YouTube), file sharing (eg DropBox), social media (eg Twitter, Facebook), and video game platforms (eg Play Station) as well.[42] Furthermore, it is interesting to note that in line with the opinion of one scholar, Large Language Models, such as ChatGPT or Bard, could be considered search engines by analogy, which in turn triggers the application of the DSA for these AI-based services as well.[43] It should be noted at the outset that there is no question that the AI Act would be applicable to Large Language Models.[44]

When it comes to 'mere conduit', 'caching', and 'hosting' services, the DSA follows the logic of the e-Commerce Directive, stipulating that these intermediary service providers are liable for the information in question, unless the provider of these services fulfils the conditions for liability exemption enshrined in the DSA.[45] Although these rules can to a great ex-

---

[36] '[Consists] of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network'. See DSA, Article 3(g)(i).

[37] '[Consists] of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request'. See DSA, Article 3(g)(ii).

[38] '[Consists] of the storage of information provided by, and at the request of, a recipient of the service'. See DSA, Article 3(g)(iii).

[39] e-Commerce Directive, Article 12 para 1, Article 13 para 1, Article 14 para 1. 'Caching' is defined more precisely in the DSA, but the underlying idea is the same.

[40] An online platform is 'a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public'. See DSA, Article 3 (i).

[41] An online search engine is 'an intermediary service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found'. See DSA, Article 3(j).

[42] Beatriz Botero Arcila, 'Is It a Platform? Is It a Search Engine? It's Chat GPT! The European Liability Regime for Large Language Models' [2023] Journal of Free Speech Law 455, 468 and 478.

[43] Search engines do not fit nicely within any definition of intermediary services presented by the DSA – and previously the e-Commerce Directive – but pursuant to the case law of the Court of Justice of the European Union and the Recitals of DSA, one can confidently argue that the DSA is indeed applicable to search engines. See Arcila (n 42) 480-483.

[44] AI Act, Articles 2-3.

[45] DSA, Article 4 para 1, Article 5 para 1, Article 6 para 1.

tent[46] also be found in the e-Commerce Directive, a number of new rules have also been adopted in the regulation.

For example, when it comes to hosting services, exemption from liability does not apply to distant contracts concluded by consumers when the information provided leads the consumer to believe that the object of the transaction is offered either directly or indirectly by the online platform.[47] Similarly, Article 7, or in other words the Good Samaritan Clause – which was entered into the text of the DSA at the request of online platforms and which might draw its inspiration from Section 230 of the US Communications Act of 1934 – is a new addition to the rules on digital services.[48] However, it should be noted that the Article corresponds to a great extent to the case law of the CJEU[49] and previous European Commission documents.[50] According to the Good Samaritan Clause, intermediary service providers will not lose their immunity from liability under Articles 4-6 simply because they 'carry out [in good faith] voluntary own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content, or take the necessary measures to comply with'[51] legal obligations. One commentator argued that this rule might incentivise general monitoring by service providers, of course on a voluntary basis. Although this might be supported by the fact that intermediaries enjoy relatively large discretion when it comes to their terms and conditions, in other words they can determine through their contractual freedom how they want to offer their services, the DSA raises some limitations as well, for instance in Recital 26, which should be applied in connection with the removal of content as well. As to the technology used in this context, automated tools and other technical solutions might be employed for such purposes, ie voluntary monitoring, but the technology exploited should be reliable enough to maintain a low error ratio.[52]

---

[46] Minor changes are noticeable in the two texts. See Sebastian Felix Schwemer, 'Digital Services Act: A Reform of the e-Commerce Directive and Much More' forthcoming in A Savin, *Research Handbook on EU Internet Law* (2022) SSRN version 7–8 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4213014> accessed 22 August 2023.

[47] DSA, Article 6 para 3.

[48] Florence G'sell, 'The Digital Services Act (DSA): A General Assessment' in Antje von Ungern-Sternberg (ed), *Content Regulation in the European Union: The Digital Services Act* (Trier Studies on Digital Law, volume 1, Verein für Recht und Digitalisierung eV, Institute for Digital Law (IRDT) 2023) SSRN version 6-7 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4403433> accessed 14 August 2023.

[49] Case C-682/18 *Frank Peterson v Google LLC and Others and Elsevier Inc v Cyando AG* ECLI:EU:C:2021:503, para 109.

[50] Folkert Wilman, 'Between Preservation and Clarification. The Evolution of the DSA's Liability Rules in Light of the CJEU's Case Law' (*Verfassungsblog*, 2 November 2022) <https://verfassungsblog.de/dsa-preservation-clarification/> accessed 23 August 2023.

[51] DSA, Article 7.

[52] Schwemer (n 46) 12; DSA, Recital 26. The DSA also highlights that '[v]oluntary actions should not be used to circumvent the obligations of providers of intermediary services '[…].' See DSA, Recital 26.

Still, the DSA shows a close resemblance to the e-Commerce Directive when it reinforces the non-obligation of general monitoring or active fact-finding.[53] It should be noted that the DSA and thus the European model for intermediary service provider liability is only one of two possible models. The other one – besides the European model – originates from the US, according to which the intermediary service provider will not be liable for information stored on the platforms, save for copyright infringements. This also means that there is no general monitoring obligation in the US. The second version of liability is a so-called conditional liability regime, which can be illustrated by the EU and the US when it comes to copyright infringements. In these cases, there is no general monitoring obligation, but once the service provider learns of the illegal content, action must be taken against it.[54] It is also interesting to note in connection with the US that the DSA might clash with US legislation, for example Texas's HB 20 law, which prohibits social media platforms from moderating speech based on speaker viewpoint.[55] Reference can also be made to China, where Article 1195 of the Civil Code of the People's Republic of China declares that the network user is jointly and severally liable if the intermediary service provider (network service in the terminology of Chinese law) does not take necessary measures after the notice of the right holder or, as laid down in Article 1197, if the service provider knows or should have known about a civil-law or interest infringement but does not take necessary measures against such actions.[56]

Turning back to the DSA, conditional liability means, for example when it comes to hosting services, that safe harbour from liability for service providers is conditioned by the lack of knowledge of the illegal activity or content – or regarding claims of damages, they are unaware of any facts or circumstances based on which illegal activity or content should be apparent – or when they indeed obtain information regarding these, they act as soon as possible to remove or disable access to the content in question.[57] Conditional liability, however, is only applicable when the service provider does not play an active role, in which it gains knowledge of or control over the information that is provided by the user, in other words, it loses its neutrality.[58] This rule can be traced back to the case law of the CJEU,[59] most prominently to *L'Oréal SA and Others v*

[53] DSA, Article 8; e-Commerce Directive Article 15.

[54] Nagy Katalin, Polyák Gábor, 'Az internetes forgalomirányító szolgáltatók működésének alapjogi vonatkozásai' [2018] 1 Jura 88, 91-92.

[55] HB20 is even more relevant, since the Fifth Circuit held the legislation constitutional. See Ioanna Tourkochoriti, 'The Digital Services Act and the EU as the Global Regulator of the Internet' [2023] Chicago Journal of International Law 129, 144-145.

[56] Civil Code of the People's Republic of China Articles 1195 and 1197.

[57] DSA, Article 6 para 1.

[58] DSA Recital 18.

[59] Wilman (n 50).

eBay International AG and Others.[60] An issue worth mentioning regarding these rules is the definition of illegal content, which is given by the DSA in Article 3(h) as

> any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law.[61]

This essentially means that any type of illegality can fall under the illegal content definition, which might change the trend for service providers, which tended to focus on criminally illegal content, while ignoring for example consumer protection law violations.[62]

In our understanding, as we go ahead in digital transformation, two aspects will become especially interesting for service providers. First, that they could help the work of the authorities in a lawful and regulated manner, thus not under the table, and, second, that they receive 'immunity' from liability in these cases.[63] Otherwise, they would lose interest in cooperating and in reducing risks in terms of exercising user rights. We believe that the lawmaker was aware of these factors and thus the DSA was drafted along these lines.

Besides norms regulating liability, the DSA also lays down due diligence obligations to achieve a transparent and safe online environment. The logic behind the DSA in this regard is the gradual approach of responsibilities, meaning that the DSA sets minimum due diligence obligations which are applicable to all intermediary service providers, then it gradually raises the number of obligations first to hosting services, then to online platforms, and finally to very large online platforms and very large search engines.[64] We believe that this regulatory approach is one of the key strengths of the DSA in comparison, for example, with the GDPR, which does not differentiate between data controllers based on their size or the risks their personal data processing poses.

As minimum level obligations, the DSA requires all intermediary service providers to designate single points of contact for communication with Member State and EU authorities[65] and for recipients of services.[66]

---

[60] Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others* ECLI:EU:C:2011:474, paras 112-113.

[61] DSA, Article 3(h).

[62] Catalina Goanta, 'Now What. Exploring the DSA's Enforcement Futures in Relation to Social Media Platforms and Native Advertising' (*Verfassungsblog,* 2 November 2022) <https://verfassungsblog.de/dsa-now-what/> accessed 23 August 2023.

[63] Lawrence A Cunningham, 'Beyond Liability: Rewarding Effective Gatekeepers' [2007] Minnesota Law Review 323, 323-326

[64] DSA, Chapter II, Sections 1-5.

[65] DSA, Article 11 para 1.

[66] ibid, Article 12 para 2.

Furthermore, service providers which do not have an establishment in the EU, but nevertheless offer services in the Union, must also designate a legal representative in one of the Member States to act as a sort of contact point with Member States and EU authorities.[67] This norm is very similar to the representative of the controllers or processors in accordance with the GDPR.[68] In addition, the DSA requires service providers to 'include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service'.[69] This information should reflect how the service provider moderates content and what kind of rights the users have.[70] Last but not least, all service providers must also publish transparency reports on their content moderation, with the exception of micro or small enterprises.[71] However, once again, such systems are not new under the sun. Meta Inc, for instance, regularly publishes its content moderation practices on Facebook and Instagram.[72] Nevertheless, such an obligation will still be a great step towards transparency for smaller – but above the micro and small business level – service providers who have not been engaged in this reporting activity so far. And it is also important to highlight that a binding reporting obligation is much better than voluntary reports in terms of content and enforceability. In conclusion, it is our understanding that the due diligence obligations of the DSA centre on consumer protection and they build on existing norms and good practice to this effect.[73]

There are other obligations that the DSA creates for hosting service providers, such as a notice and action mechanism for users,[74] and notification of the authorities of the Member States in the case of suspicion of criminal offences which would involve an actual or possible threat to the life or safety of a person.[75] Further responsibilities are placed on online platforms, such as the obligatory establishment of an internal complaint-handling system,[76] supplemented by an out-of-court settlement

[67] ibid, Article 13 paras 1-2.

[68] GDPR, Article 27.

[69] DSA, Article 14 para 1.

[70] ibid.

[71] DSA, Article 15 paras 1-2. A small enterprise is an enterprise which employs fewer than 150 persons, and its annual balance sheet and/or its turnover is less than EUR 10 million. A micro enterprise is even smaller than that. See Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L123, Article 2 paras 2-3. It should also be noted that online platforms and very large online platforms, and very large search engines have their own transparency reporting obligations.

[72] See Community Standards Enforcement Report Q1 2023 <https://transparency.fb.com/reports/community-standards-enforcement/> accessed 17 August 2023.

[73] See, for example, e-Commerce Directive, Article 10.

[74] DSA, Article 16.

[75] ibid, Article 18.

[76] ibid, Article 20.

mechanism,[77] and many more, for instance the compliance by design obligations of those online platforms which allow users to conclude distant contracts with traders on their platform.[78] This norm is fairly similar in its nature and goal to the data protection by design and by default rules of the GDPR.[79] The internal complaint-handling system and the out-of-court settlement mechanism can be seen as an excellent way to tackle the problem observed by one commentator, namely that in our information dependent and driven societies, social media platforms act as gatekeepers, and thus they have the power to fundamentally affect political discourse. A good example of this is when Twitter permanently suspended the account of Donald Trump, former US president, without any judicial or independent review.[80] It is important to highlight in connection with this that review cannot be made solely by automated means. In other words, while taking down content can be automated, the review of such a decision cannot.[81]

Last but not least, the DSA created a special framework of rules for VLOPs and VLOSEs. An online platform or a search engine can turn into a VLOP or a VLOSE when the number of average monthly active users of the service in the EU reaches 45 million and when the European Commission designates the providers as such.[82] The European Commission announced the list of VLOPs and VLOSEs for the very first time on 25 April 2023, designating 17 VLOPs and only 2 VLOSEs. To name a few examples of each, VLOPs include the usual suspects, such as Facebook, Instagram, TikTok and YouTube, but one can find surprises on the list as well, for example Zalando or Wikipedia. On the other hand, VLOSEs produce no bewilderment, as Bing and Google were designated as such.[83]

When it comes to VLOPs and VLOSEs, the DSA creates obligations which will cause a serious financial burden and commitment from these service providers. One of the new obligations is risk assessment related to their services and the systems they use, and the connected risk mitigation requirement.[84] Once again, similarities can be identified with the GDPR's data protection impact assessment rules.[85] Another important rule is the so-called 'crisis response mechanism', which is triggered if 'extraordinary

[77] ibid, Article 21.

[78] ibid, Article 31.

[79] GDPR, Article 25.

[80] Giancarlo Frosio, 'Platform Responsibility in the Digital Services Act: Consitutionalising, Regulating and Governing Private Ordering' forthcoming in Andrej Savin and Jan Trzaskowski (eds), *Research Handbook on EU Internet Law* (Edward Elgar) 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4236510> accessed 22 August 2023.

[81] Schwemer (n 46) 15.

[82] DSA, Article 33 para 1.

[83] European Commission, 'Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines' (press release, 25 April 2023) <https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413> accessed 18 August 2023.

[84] DSA, Articles 34-35.

[85] GDPR, Article 35.

circumstances lead to a serious threat to public security or public health in the Union or in significant parts of it'.[86] In such cases, the European Commission may require service providers to act in accordance with the decision of the Commission.[87] A great financial burden is also introduced in the form of an annual audit to assess compliance primarily with the due diligence obligation of the DSA.[88] One cannot but wonder whether this is also part of the 'hidden' European agenda on strengthening the compliance and audit industry, something that started with the GDPR – with the extensive, and expensive privacy audits that full compliance usually requires – followed by the NIS 2 Directive – with, for example, regular and targeted security audits on essential entities.[89] Another part of the new financial burden is the supervisory fee that the Commission charges these organisations.[90] The good news for the rest of the industry is that these obligations are only applicable to VLOPs and VLOSEs. An interesting question for the future is whether service providers close to the 45 million user border will try to decrease their user base in Europe to escape these robust obligations, or if this will deter them from engaging with their EU audience. This is especially curious considering recent threats from Meta to 'pull out' of Europe in light of the difficulties of data transfer from the EU to the US based on the GDPR.[91] If service providers choose to move away from Europe because of the DSA's obligations, then this will certainly prove disadvantageous for many European consumers.

Finally, it is also useful to summarise the enforcement system and mechanism of the DSA. First, the DSA requires Member States to designate one or more competent authorities to supervise the enforcement of the regulation, one of which should be a Digital Services Coordinator (DSC).[92] In Hungary, the tasks of the DSC were taken by an existing governmental agency, namely the National Media and Infocommunications Authority.[93] DSCs generally have two types of competencies: investigative and enforcement, related, for instance, to requiring information from ser-

---

86 DSA, Article 36 para 2.

87 ibid, Article 36 para 1.

88 ibid, Article 37.

89 NIS 2, Directive Article 32 para 2(b).

90 DAS, Article 43.

91 Pascale Davies, 'Meta Warns It May Shut Facebook in Europe but EU Leaders Say Life Would Be "Very Good" Without It' (*Euronews*, 7 February 2022) <https://www.euronews.com/next/2022/02/07/meta-threatens-to-shut-down-facebook-and-instagram-in-europe-over-data-transfer-issues> accessed 18 August 2023. Meta later refuted the news. See Marksu Reinisch, 'Meta Is Absolutely Not Threatening to Leave Europe' (*Meta*, 8 February 2022) <https://about.fb.com/news/2022/02/meta-is-absolutely-not-threatening-to-leave-europe/> accessed 18 August 2023. This issue nevertheless seems to be resolved for the time being with the adoption of the new Privacy Framework. See European Commission, 'Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows (Press release, 10 July 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721> accessed 18 August 2023.

92 DSA, Article 49 paras 1-2.

93 The designation was made by Act LXI of 2022, Section 24 para 1.

vice providers, or to carrying out inspections and/or to imposing fines.[94] Member States have been granted the power to create national legislation on penalties for infringement of the DSA, with the limitation that fines for a breach of an obligation cannot exceed 6% of the annual worldwide turnover of the preceding financial year of the service provider, and this threshold is considerably lower, 1% of the annual turnover, if the breach is 'procedural' in nature, eg supplying wrong information. For periodic penalty payments, the fine should be no more than 5% of the average daily worldwide turnover or income in the last fiscal year.[95]

The DSA also sets up a European Board of Digital Services (EBDS) which is an advisory body made up of DSCs and the European Commission (as chair).[96] The Board was tasked with supporting the DSCs, among other ways, in the form of issuing opinions and recommendations.[97] In addition, the European Commission may also exercise supervisory powers in the case of VLOPs and VLOSEs, including the right to impose financial sanctions according to the above-mentioned logic.[98] In this latter case, the CJEU gained competence to review such decisions from the Commission.[99]

One cannot but find similarities once again with existing secondary and interestingly primary EU legislation. The GDPR also requires Member States to designate supervisory authorities,[100] uses a similar method for determining the maximum amount of fines,[101] and creates the European Data Protection Board composed of Member State supervisory authorities and the European Data Protection Supervisor, with similar tasks to that of the EDBS.[102] It should also be highlighted in connection with the GDPR that, according to one commentator, the European Commission may face difficulties in terms of remaining uninfluenced in its enforcement powers, given the Commission's role in the making of secondary EU law. It might be possible that the Commission's own policy decisions in other fields, such as data protection, could influence the organisation's supervisory powers.[103] A further interesting parallel can also be drawn between penalty payments in the DSA and in the TFEU imposed by the CJEU on Member States for treaty infringement.[104]

---

94 DSA, Article 51 paras 1-2.

95 ibid, Article 52.

96 ibid, Article 61 para 1 and Article 62 paras 1-2.

97 ibid, Article 63.

98 ibid, Article 65ff.

99 ibid, Article 81.

100 GDPR, Article 51.

101 ibid, Article 83.

102 ibid, Articles 68 and 70.

103 Ilaria Buri, 'A Regulator Caught Between Conflicting Policy Objectives. Reflections on the European Commission's Role as DSA Enforcer' (*Verfassunsblog,* 31 October 2022) <https://verfassungsblog.de/dsa-conflicts-commission/> accessed 23 August 2023.

104 Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/260, para 2.

3 The Digital Markets Act

The DMA is by its very name an attempt to regulate the markets affected by the digital sector. The regulation sets out its requirements in six chapters and 109 recitals. The legislation is closely linked to the issue of promoting digitalisation and supporting it through legal instruments.[105] At the heart of this regulation lies the problem of gatekeepers, which in the end can create 'serious imbalances in bargaining power and, consequently, unfair practices and conditions for business users, as well as for end users of core platform services provided by gatekeepers, to the detriment of prices, quality, fair competition, choice and innovation in the digital sector'.[106]

Access to the certain fundamentally important services takes place through various service providers, among which online platforms and search engines play key roles. This role has already been described in scholarship by the term gatekeeper.[107] Gatekeepers have long been addressed by European legislation,[108] as they have the ability to influence the decisions and perceptions of their users. Gatekeepers as defined by the DMA are providers of core platform services, such as online search engines like Google or Bing, video-sharing platform services like TikTok, operating systems like macOS, and many more, including web browsers, virtual assistants, cloud services, and online advertising services.[109] The scope of the DMA, therefore, covers not only services in the online digital space, but also software solutions installed on computers that can operate offline. A number of these core platform services are also classified as intermediary services, as already mentioned in connection with the DSA.[110] This broad definition helps to ensure that all gatekeeper services that have the potential to significantly influence users' decisions would fall under the scope of the DMA, but it also requires that they have a significant impact on the internal market, that the service they provide is a genuinely important gateway for business users to reach end users, and that their market position is sufficiently stable to justify compliance with the higher requirements.[111] In this respect, as already mentioned above, the regulation makes gatekeeper status conditional on financial performance within the EU and on the 45 million monthly active end users, at

[105] Jörg Hoffmann, Liza Herrmann and Lukas Kestler, 'Gatekeeper's Potential Privilege: The Need to Limit DMA Centralization' [2023] Journal of Antitrust Enforcement 1.

[106] DMA, Recital 4

[107] Rikke Frank Jørgensen, 'Human Rights and Private Actors in the Online Domain' in Molly K Land and Jay D Aronson (eds), *New Technologies for Human Rights Law and Practice* (CUP 2018) 249, 251.

[108] Rupprecht Podszun and Philipp Bongartz, 'The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers' [2021] Journal of European Consumer and Market Law 60, 61-62.

[109] DMA, Article 2 paras (1)-(2).

[110] ibid, Article 2.

[111] ibid, Article 3, cf DSA Article 33 para 1.

least for the duration of three financial years, bringing its rules closer to the definition of VLOPs and VLOSEs in the DSA.[112]

Since these services are typically provided from outside the EU, the regulation has a clearly stated objective to bring these gatekeepers based in third countries under its scope and to regulate the operational framework for the services they provide.[113] In examining the implications of the regulation for digitalisation, it is therefore particularly appropriate to examine the scope issues for the following reasons. The reason for granting a higher degree of protection, circumscribed by public law rules,[114] is that the legal relationship between the end user and the service provider based on the principles of civil law, thus one party, in this case core platform service providers, will have a significant advantage compared to their users, the 'consumers'.[115] The legal relationship becomes perceptibly one sided in the sense that one party, the undertaking, is in a better position to assert its interests and, in a critical situation, can exercise strong independent influence on the development of the legal relationship and the resulting disputes, irrespective of the interests and expectations of the other party, which can otherwise be considered legitimate. This is also pointed out in Recitals 4 and 13 of the DMA, when it provides for the protection of European citizens and digital businesses against services provided by large third-country companies on unfair and one-sided terms.

To this end, the regulation applies extraterritorially, similar to the DSA: the extraterritorial scope in this case means that the scope of the regulation, and thus the enforcement rights of end users, also extend in certain aspects to the activities and services of gatekeepers and platform providers not resident in the EU. This creates a win-win situation for end users and business users alike, as they can apply EU rules to the legal relationship and only have to partially adapt to the requirements of the legal regime linked to the nationality of the gatekeepers operating the platforms.[116] This is yet again an example of the above-mentioned Brussels effect.

In the event of a dispute, European consumers will be able to pursue their claims under rules that are favourable to them, as jurisdiction and competence will not be based on the domicile of the claimant or, in other words, the gatekeeper, but rather on the domicile or residence of the

---

[112] DMA, Article 3 para 2.

[113] ibid, Recital 13.

[114] Pierre Bourdieu, 'The Force of Law: Toward a Sociology of the Juridical Field' [1987] Hastings Law Journal 805, 814-818; Thomas Livolsi, 'Scope of the e-Commerce Directive 2000/31/EC of June 8, 2000' [2001] Columbia Journal of the European Law 473.

[115] Not all users of such services will necessarily be consumers as defined by consumer protection laws, such as those businesses which operate largely or exclusively on online platforms.

[116] Caroline Cauffman and Catalina Goanta, 'A New Order: The Digital Services Act and Consumer Protection' [2021] European Journal of Risk Regulation 758, 758-765.

consumer (end user or business user).[117] This is also reflected in Article 1 paragraph 2 of the DMA, according to which the rules of the regulation apply to platform services provided by gatekeepers, regardless of their place of establishment, residence, or the applicable law otherwise governing the service. Thanks to the above provision, gatekeepers will not be able to contract out of the scope of the DMA by choosing the governing law of the contract, so even if they choose to apply the law of a non-EU third country as the governing law of the general conditions of their services, the requirements of the DMA will still apply to the resulting legal relationship.

It is important to note, however, that this system can be fragile: extraterritorial application seems to offer great potential for EU enforcement bodies and more effective protection for European consumers against businesses providing services from outside the EU, but experience so far shows a different picture. The application of the GDPR highlights the problem of practical applicability, which, in spite of the Brussel effect, may prevent the enforcement of the regulation's requirements.[118] This means that gatekeeping services are of such economic importance to the EU that the application of EU legislation containing strict requirements may be blocked or severely hindered when it is implemented and when Member State enforcement bodies impose sanctions based on non-compliance with those requirements.[119] Large third-country companies may face interminable legal procedures and political pressure, and in many cases the companies concerned simply do not implement the requirements imposed on them, do not cooperate with the authorities, and this may substantially weaken the applicability of further Union legislation. This impact is not insignificant and can only be resolved if the enforcement bodies – EU and Member State alike – apply the law in a uniform and consistent way and support national authorities in doing so.

The DMA, after setting out the criteria for designation as a gatekeeper in Chapter II, lays down the notification obligation for potential gatekeepers and then addresses the specific requirements that gatekeepers must meet.

One way of ensuring this is to create a notification obligation for gatekeeper services: if service providers reach the thresholds for designation as gatekeepers, as outlined above, they must notify the Commission and send them the necessary information for designation. In this notification, the undertaking concerned must clearly identify the services for

[117] Chiarella (n 4) 33.

[118] Dan Jerker B Svantesson, 'Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation' [2015] International Data Privacy Law 226.

[119] Joanne Scott, 'Extraterritoriality and Territorial Extension in EU Law' [2014] The American Journal of Comparative Law 87, 88; See Renzo Marchini, Camille Ebden and Alex Beresford, 'Meta Transfer Enforcement from the Irish DPC: Issues and Consequences for Other Companies' (*fieldfisher*, 23 May 2023) <https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/meta-transfer-enforcement-from-the-irish-dpc> accessed 25 August 2023.

which the thresholds are reached.[120] In the absence of a notification, the Commission can also proceed with the designation, against which the undertaking concerned can demonstrate that, although the core platform service meets all the conditions, it exceptionally does not meet the requirements listed in Article 3 paragraph 1 due to the operational circumstances of the core platform services concerned.[121]

On the basis of the requirements of the regulation, the Commission must establish a designation decision specifying the relevant platform services as gatekeepers and the obligations on them as set out in Article 5. As of writing, there are seven potential gatekeepers, such as Alphabet, Apple, Microsoft – the usual suspects – but interestingly Samsung as well.[122]

A significant part of the requirements, which are defined in Chapter III DMA, is designed to prevent gatekeepers from gaining further benefits by pooling and jointly using the data sets they have acquired through their services – in accordance with Recitals 2 and 13 DMA. On this basis, it is prohibited to combine data with personal data obtained from other services, and to circulate data used in the provision of one of its services in the provision of another service, even by inducing its users to use another service, except if the user gives his or her consent to the processing.[123] These requirements are intended to reduce the ultimate bargaining power of the gatekeeper, as these gatekeepers may appear as a single solution for certain services, single, big platforms that may become inescapable, thereby worsening competition in the EU internal market, leaving both end users and business users connecting through the platform service vulnerable. However, it is questionable whether the requirements of the regulation can be exempted from these prohibitions[124] if the end user has been offered a specific choice and has given his or her consent under the requirements of the GDPR.

While this may seem to give back choice to users, this is really only an illusion, as the legal basis for the provision of services is more likely to be the legal basis for the performance of the contract,[125] leaving users with only the illusion of consent, which can be a significant market influencing force. It should therefore be pointed out that this problem is only apparent, yet it has an impact on user decisions. The very nature of platform services means that this may not be a real alternative for users, and leaves them in a similar dilemma as before the GDPR: for immediate

[120] DMA, Article 3 para 3.

[121] ibid, Article 3 para 5.

[122] 'Remarks by Commissioner Breton: Here Are the First 7 Potential "Gatekeepers" under the EU Digital Markets Act (*European Commission*, Statement, 4 July 2023) <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_23_3674> accessed 25 August 2023.

[123] DMA, Article 5 para 2.

[124] ibid.

[125] GDPR, Article 6.1(b).

benefits (platform use, easy access to acquaintances, and so on), they are more willing to sacrifice the protection of their data than consider the more distant and indirect disadvantages (data theft, incidents and disadvantages resulting from data interlinking, profiling) as a real risk. The cognitive and structural problems outlined by Daniel J Solove are revived here.[126] The article will turn back to this issue below.

However, this situation is mitigated by the introduction of rules such as the audit obligation outlined in Article 15 DMA, whereby the gatekeeper is obliged to present its profiling techniques to the Commission, which may adopt audit rules on them in an implementing act. This will allow the EU institution to have a meaningful insight into the technical solutions, preventing the disadvantages of using some methods.

The other direction of the key requirements for gatekeepers is that the rights of business users who use the platform service to provide their own services also enjoy heightened protection. For instance, gatekeepers cannot arbitrarily favour their own products and services, impose mandatory use of their own systems, or require subscription or registration to other services.[127] These requirements will also make it easier for business users to switch platforms and gatekeepers, creating a higher level of competition in the market for platform services.

This approach is also reflected in the requirements for inter-personal communications services, where interoperability requirements make it easier for business users to connect to the services of the provider and a liberalisation direction can be seen with the reference offer and other obligations under Article 7, the regulatory direction of which is very similar to the way the EU legislator previously sought to facilitate the opening of markets dominated by State monopoly telecom operators through liberalisation in order to create a single internal market.[128]

From a digitalisation point of view, the provisions under which gatekeepers must allow end users more freedom than before in terms of IT settings under the DMA are of great importance. Where there is an end-user relationship with a gatekeeper described above, this means that the end user is given complete freedom to change the default settings of the gatekeeper's operating system, virtual assistant, or web browser, within certain well-defined limits that guide or direct end users to products or services offered by the gatekeeper, or to easily remove software applications installed on the gatekeeper's operating system that are not essential for the operation of the service, operating system, or device.[129]

---

[126] Daniel J Solove, 'Introduction: Privacy Self-management and the Consent Dilemma' (2012) 126 Harv L Rev 1880.

[127] DMA, Article 5 para 8.

[128] Damien Geradin, 'Twenty Years of Liberalization of Network Industries in the European Union: Where Do We Go Now?' [2006] SSRN version < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=946796> accessed 18 August 2023.

[129] DMA, Article 6 para 3.

Similarly, taking forward the outcome of the earlier decryption debate,[130] it should allow the installation and effective use of third-party software applications or app stores containing them, providing the access and information necessary for interoperability.[131]

These requirements allow consumers who are end users to tailor these services to their own needs and to combine them with other services they use. The requirements clarify and provide a framework for the digital copyright developments of the last decades, which both third-party software developers and end users will benefit from, in comparison to the entrenched and long-lasting position of the gatekeeper service providers.

The DMA also requires gatekeepers to provide end users with access to and use of content, subscriptions, features, or other items through the business user's software application, even if those items were obtained from the relevant business user without the use of the gatekeeper's core platform services.[132] This indeed ensures the user's freedom of choice, regardless of the settings of the basic platform services of the gatekeeper, and also contributes to the user's ability to fulfil and enjoy the consumer legal relationship to the fullest extent possible.

The gatekeeper must also ensure the portability of data for users, thus enabling them to switch providers, even if this process may be difficult when the data are delivered.[133] The difficulty lies in the fact that the data are organised according to the capabilities and system of the original gatekeeper, hence even if the data are in an open file format, their usability can be severely hindered. If we look at the regulatory objective, it is therefore rather the objective of ensuring the interoperability of data that lies behind the requirement to provide the possibility to switch between service providers.[134] Data management is also considered a key regulatory issue: Article 5(2) DMA sets out the conditions for the use of end users' data, which are designed to prevent gatekeeping services from gaining an unfair advantage in the market simply because their services are widely used by users, making it difficult for them to switch providers in the event of a data breach. To this end, it must not process or combine the personal data of end users who use a third-party service operating

---

[130] Case T-167/08 *Microsoft Corp v Commission* ECLI:EU:T:2012:323. The controversy was based on the fact that operating system vendors in the early years of computing did not allow unrestricted access to the source code of their systems, which had a restrictive effect on competition in the software development market. The dispute was resolved by the judicial declaration of an interoperability obligation, and we see its continuation in these requirements. See Jonathan Band, *Interfaces on Trial: Intellectual Property and Interoperability in the Global Software Industry* (Routledge 2019) 50-62.

[131] DMA, Article 6 para 7.

[132] DMA, Article 5 para 5.

[133] Antonio Manganelli and Antonio Nicita, 'Regulating Big Techs and Their Economic Power' in Antonio Manganelli and Antonio Nicita (eds), *Regulating Digital Markets: The European Approach* (Springer International Publishing 2022) 137-165.

[134] See Jörg Hoffmann and Begona Gonzales Otero, 'Demystifying Data Interoperabilty in the Access and Sharing Debate' [2021] JIPITEC 252.

on the gatekeeper's services, use data obtained through the gatekeeper's platform services for other services, and enter end users into contracts for other services of the gatekeeper for the purpose of combining personal data.[135]

For both business users and end users, the DMA regulation creates the right to raise 'any issue of non-compliance with the relevant Union or national law by the gatekeeper with any relevant public authority, including national courts, related to any practice of the gatekeeper'.[136] This is an option that is always available, even under different contractual terms and conditions, which serves as an addition to legitimate internal or extra-judicial dispute resolution mechanisms, for the enforcement of consumer rights and services. However, it does not include the consumer's right to turn to the national authorities to enforce the provisions of the DMA, as this is excluded by Article 1(5) DMA.[137]

Under Article 8 of the Regulation, the gatekeeper must not only ensure but also be able to demonstrate compliance with the requirements set out in the DMA. This is very similar to the principle of accountability of the GDPR.[138] The Commission may initiate a procedure to find whether the gatekeeper is compliant or adopt an implementing act specifying the measures to be taken by the gatekeeper to achieve compliance with the requirements applicable to it. The requirements for this procedure are set out in Chapter IV of the DMA. The gatekeeper can request such a procedure from the Commission as well.[139]

The Commission has wide-ranging powers in the procedure, not only to request information from the gatekeeper,[140] but also to carry out interviews and take statements,[141] and even to carry out on-the-spot inspections if it considers them justified.[142] Where investigations show that there is a risk of serious and irreparable harm to the business users or end users of gatekeepers, the Commission may take interim measures, including by means of implementing acts.[143] If the investigation reveals non-compliance, the Commission will have more tools than before to encourage gatekeepers to comply: it may impose a fine, which may be substantial, up to 10% of the gatekeeper's total worldwide turnover in

[135] See Szőke Gergely László and Pataki Gábor, 'Az online személyiségprofilok jelentősége' in Polyák Gábor (ed), *Algoritmusok, keresők, közösségi oldalak és jog – A forgalomirányító szolgáltatások szabályozása* (HVG ORAC 2020) 79-88.

[136] DMA, Article 5 para 6.

[137] See Josef Drexl and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 2 May 2023 on the Implementation of the Digital Markets Act (DMA)' [2023] GRUR International Volume 864, 866-867.

[138] GDPR, Article 5 para 2.

[139] DMA, Articles 8 and 20.

[140] ibid, Article 21.

[141] ibid, Article 22.

[142] ibid, Article 23.

[143] ibid, Article 24.

the previous financial year,[144] and, in addition, in the event of failure to comply or systematic non-compliance with the measures ordered by the Commission, a periodic penalty payment,[145] which may be imposed on the undertaking and its associations from the date specified in the decision, up to 5% of their average daily worldwide turnover in the previous financial year until the obligation is fulfilled. It should be added that this is the *ultima ratio* sanction of the remedy system outlined in the DMA, and the Commission has a number of enforcement tools at its disposal. The similarities of this method to the DSA and other above-mentioned instruments are noteworthy. While a gatekeeper can avoid negative legal consequences by offering commitments,[146] or by cooperating with the Commission's preliminary findings,[147] in their absence the Commission is given explicitly strong powers to ensure enforcement, which can also act as a deterrent to more serious infringements. Cooperation between the Commission and the national authorities and courts of the Member States is also facilitated by strong cooperation under the requirements of the regulation, which is capable of outlining a uniform European enforcement process to help ensure that gatekeeper companies cannot hide behind the laws of any EU Member State in the case of non-compliance.[148]

However, it should also be emphasised in this respect that this cooperation should be based on a strict delimitation of competences. It is obvious that the implementation of the DMA could be undermined by the introduction of differentiated national implementation mechanisms.[149] Therefore, it is important that no additional obligations should be imposed on gatekeepers under national law, as this could also hinder the 'Union' characteristic of the regulation. This will ensure the uniform application of the DMA, which will help the digitalisation process to move forward in the internal market.

4 Conclusions

The development of digital technologies and the age of platforms require an appropriate legal framework and aptitude from the legislator – and this is particularly true when we think of legislation at the European level. Digital services, gatekeepers, intermediaries, and content providers are now pervading much of and actively shaping the social and economic aspects of our lives. One of the major dilemmas in regulating these areas is how to create a technology neutral, and therefore timeless, regulatory framework that provides the appropriate basis for the parties concerned to further regulate their own legal relationships, on which services can

144 ibid, Article 30.

145 ibid, Article 31.

146 ibid, Article 25.

147 ibid, Article 29 paras 2-6.

148 ibid, Articles 37-39.

149 Hoffmann, Herrmann, Kestler (n 105) 6-7.

be based, even at the global level, while at the same time fully protecting the rights and legitimate interests of consumers, users, and other stakeholders.

The DSA and DMA in this respect regulate a long-standing problem in relation to the services provided by gatekeepers and intermediaries, which by the nature of things have a disproportionate advantage in their legal relationship with their users, which warrants further protection for these groups and specific responsibilities for the intermediaries and gatekeepers. The analysis carried out shows that, in addition to the existing requirements, the DSA and DMA have created new obligations for service providers which create better conditions both in the area of fair competition and in the area of consumer relations, but still they do not fundamentally change the liability regime of intermediary service providers. This does not mean, however, that the DSA and DMA would have only advantages, to which the chapter returns in the last paragraph.

The regulations represent a significant step forward in harmonising legislation among Member States, and they strengthen the extraterritorial applicability of EU law, depicted as the Brussels effect. Enforcement of the two regulations is fairly similar to the approach of the GDPR, but they place more emphasis on the role of the European Commission than national supervisory authorities. This, combined with the significant scope for intervention and the high level of fines, will create a more uniform application of the law and could provide a meaningful deterrent to non-compliance. As has been repeatedly pointed out in the article, the DSA and the DMA follow in the footsteps of a handful of recent and earlier secondary legislation in the field, but the similarities to the GDPR – and of course the e-Commerce Directive – are the most striking. The regulations also draw inspiration from best practices in the industries as shown above for instance on the reporting obligations.

The various solutions for transparency activities (reporting, internal complaints handling with users, etc), which have so far been carried out on a voluntary basis, will become mandatory rules that can serve the development and progress of the whole sector and help digitalisation to move forward by imposing uniform requirements on all market players, albeit with a layered set of requirements.

However, there are also serious concerns about the requirements: it is feared that the strengthened enforcement rules will increase operational costs for service providers, thus creating a barrier to entry to the markets. This might not be significant for VLOPs and VLOSEs,[150] since a barrier to the market usually benefits existing actors on the market, but this may very well produce side effects in Europe, where startups might

[150] The cost of non-compliance in their case, however, is very significant. Alphabet, for instance can have a maximum yearly fee of USD 76 million based on the DSA alone. These data are based on the 2021 financial year. See Afiq Fitri, 'Europe's Digital Services Act Is Set to Cost Big Tech Millions' (*Tech Monitor*, 6 April 2022) <https://techmonitor.ai/policy/big-tech/digital-services-act-cost-eu-alphabet-meta> accessed 31 August 2023.

be persuaded to avoid the continent, based on a cost-benefit analysis.[151] Since the DMA does not apply to small and medium-size businesses, this conclusion is relevant only to the DSA. It needs to be noted, however, that according to PwC, the DSA and the DMA might contribute to better competition through lowering the Herfindahl-Hirschman Index, by creating low barriers to entry.[152] While this is certainly true regarding national law fragmentation in the field, which is solved by the DSA and DMA, the DSA still operates with complex compliance obligations that will heighten entry barriers in comparison with other parts of the worlds.

This will put EU users at a disadvantage in the digitalisation process, since they might lose the opportunity to use new and innovative services based on the operational demands of startups highlighted above. This is due to an EU disadvantage vis-à-vis competitors from third countries, which could operate without such compliance burdens. On the one hand, this could disrupt economic processes in the EU by not facilitating but hindering the future establishment of digital services businesses in the EU, and, on the other hand, it could isolate European users from the latest digital solutions and platform services, which in any case are the result of a slow process. These conclusions remain valid, even though the DSA and the DMA should be praised for their layered approach – especially when it comes to the DMA – which is a significant step forward from the GDPR's generalised compliance costs put on small businesses and giants alike.

Suggested citation: B Hohmann and B Kis Kelemen, 'Is There Anything New Under the Sun? A Glance at the Digital Services Act and the Digital Markets Act from the Perspective of Digitalisation in the EU' (2023) 19 CYELP 225.

[151] Adam Hays, 'Barriers to Entry: Understanding What Limits Competition' (*Investopedia*, 28 September 2023) <https://www.investopedia.com/terms/b/barrierstoentry.asp> accessed 19 October 2023.

[152] The Digital Services Acts Package and What It Entails (*PwC*) <https://www.pwc.com/m1/en/publications/documents/the-digital-services-acts-package.pdf> accessed 19 October 2023.